**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ПРИРОДОКОРИСТУВАННЯ**
**ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**
**КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

# КВАЛІФІКАЦІЙНА РОБОТА

другого (магістерського) рівня вищої освіти

на тему: «Підвищення ефективності безпечної передачі даних в пристроях інтернету речей»

Виконав: здобувач 6 курсу гр. Іт-62

Спеціальність 126 «Інформаційні системи та технології»

Лопатюк Микола Сергійович

Керівник: Шувар Б.І.

Рецензент: _____

**ДУБЛЯНИ-2024**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ПРИРОДОКОРИСТУВАННЯ
ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Другий (магістерський) рівень вищої освіти
Спеціальність 126 «Інформаційні системи та технології»

«ЗАТВЕРДЖУЮ»
Завідувач кафедри

_____
(підпис)

д.т.н., проф. А.М. Тригуба
___ _____ 2024 р.

**ЗАВДАННЯ**

на кваліфікаційну роботу здобувачу

Лопатюк Микола Сергійович

1.Тема роботи: «Підвищення ефективності безпечної передачі даних в пристроях інтернету речей»
керівник роботи к. е н., доцент, Шувар Б.І.
затверджені наказом Львівського НУП № 616/к-с від 12.09.2024р.
2. Строк подання студентом роботи 29.11.2024 р.
3. Вихідні дані до роботи: Технічні вимоги до пристроїв Інтернету речей для безпечної передачі даних. Програмна конфігурація IoT-системи, включаючи параметри енергоспоживання та захисту даних. Науково-технічна і довідкова література з тематики безпеки та енергоефективності в IoT. Результати експериментальних досліджень та тестів впливу впроваджених рішень на енергоефективність.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)
1. Аналіз стану питання в теорії та практиці. 1.1. Теоретичні основи безпеки передачі даних в IoT. 1.2. Огляд сучасних протоколів та стандартів IoT. 1.3. Безпечні конфігурації пристроїв та шлюзу IoT. 2. Обґрунтування, вибір та реалізація інструментарію вирішення задачі. 2.1. Вибір технологій та методів захисту даних в IoT. 2.2. Обґрунтування архітектури системи безпечної передачі даних. 2.3. Реалізація запропонованого рішення. 2.4. Підвищення безпеки за допомогою методів машинного навчання. 3. Результати вирішення задачі. 3.1. Тестування безпечної передачі даних. 3.3. Рекомендації щодо подальшого розвитку. 4. Охорона праці та безпека у надзвичайних ситуаціях. 4.1. Охорона праці. 4.2. Безпека у надзвичайних ситуаціях. 5. Визначення ефективності. 5.1. Аналіз результатів

тестування ефективності. 5.2. Оцінка ефективності системи. Висновки та пропозиції. Список використаних джерел.

5. Перелік ілюстраційного матеріалу (з точним зазначенням обов'язкових схем та моделей): рисунки, таблиці у вигляді презентації

6. Консультанти з розділів:

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | | Відмітка про виконання |
|---|---|---|---|---|
| | | завдання видав | завдання прийняв | |
| 1, 2, 3,5 | Шувар Б.І., доцент кафедри ІТ | 16.09.2024р. | 16.09.2024р. | |
| 4 | Городецький І.М., доцент кафедри управління проектами та безпеки виробництва | 17.09.2024р. | 17.09.2024р. | |

7. Дата видачі завдання 16.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів дипломної роботи | Строк виконання етапів роботи | Відмітка про виконання |
|---|---|---|---|
| 1 | Отримання завдання. Вивчення рекомендованої літератури по темі роботи. Написання першого розділу. | з 16.09.24 | |
| 2 | Виконання другого розділу та аркушів ілюстративного матеріалу до нього | до 05.10.24 | |
| 3 | Виконання третього розділу та аркушів ілюстративного матеріалу до нього | до 15.10.24 | |
| 4 | Написання розділу «Охорона праці та безпека у надзвичайних ситуаціях» | до 22.10.24 | |
| 5 | Оцінка ефективності запропонованої системи | до 05.11.24 | |
| 6 | Завершення оформлення розрахунково-пояснювальної записки та аркушів ілюстративного матеріалу | до 20.11.24 | |
| 7 | Завершення роботи вцілому | 29.11.2024 | |

Студент _____ Лопатюк М.С.
( підпис ) (прізвище та ініціали)

Керівник роботи _____ Шувар Б.І.
( підпис ) (прізвище та ініціали)

УДК 004.42 : 004.5

Підвищення ефективності безпечної передачі даних в пристроях інтернету речей. Лопатюк М.С. Кафедра ІТ – Дубляни, Львівський НАУ, 2024.

Кваліфікаційна робота: 64с. текст. част., 11 рис., 41 джерело.

Мета роботи – розробка та впровадження ефективних підходів до забезпечення безпеки передачі даних в пристроях Інтернету речей (IoT), з урахуванням обмежень по енергоспоживанню та обчислювальних потужностях пристроїв.

Завдання дослідження: вивчення існуючих технологій безпечної передачі даних у системах IoT. Аналіз існуючих методів шифрування та автентифікації для IoT-пристроїв. Розробка оптимізованих методів для забезпечення безпеки даних з мінімальними витратами енергії. Створення моделі та методів забезпечення надійної передачі даних в умовах обмежених ресурсів пристроїв. Оцінка ефективності розробленої системи.

Об’єкти дослідження – методи шифрування, протоколи безпеки, алгоритми для забезпечення передачі даних у середовищі IoT.

Предмет дослідження – технології та алгоритми безпечної передачі даних в пристроях Інтернету речей.

Ключові слова: Інтернет речей (IoT), безпека даних, шифрування, протоколи безпеки, енергоефективність, моделювання, алгоритми, передача даних.

# ЗМІСТ

# ВСТУП

Розвиток технологій Інтернету речей (IoT) докорінно змінив сучасний світ, відкриваючи нові можливості для автоматизації, обміну інформацією та оптимізації бізнес-процесів. IoT об'єднує фізичні пристрої в єдину мережу, дозволяючи їм взаємодіяти між собою, збирати, обробляти та передавати дані. Однак, стрімке поширення IoT підвищило ризики кіберзагроз, зокрема, стосовно безпеки передачі даних.

Серед ключових викликів безпеки в IoT варто виділити проблеми автентифікації, шифрування, управління доступом та захисту від атак. Невідповідність традиційних рішень вимогам IoT, зокрема щодо енергоефективності та обмежених ресурсів пристроїв, вимагає пошуку нових підходів до забезпечення безпеки.

В рамках цієї роботи досліджується актуальне питання підвищення ефективності передачі даних в IoT шляхом розробки інноваційних рішень, які забезпечують високий рівень безпеки при мінімальних витратах ресурсів.

Мета дослідження — розробка та впровадження архітектури системи безпечної передачі даних для пристроїв IoT, яка забезпечує оптимальне поєднання безпеки, продуктивності та енергоефективності.

У роботі вирішуються наступні завдання:

- аналіз стану питання в теорії та практиці;
- ідентифікація основних проблем та формулювання завдань дослідження;
- розробка і впровадження запропонованого рішення;
- оцінка ефективності системи на основі тестування та аналізу.

Практична цінність роботи полягає у створенні ефективного інструментарію для захисту передачі даних в IoT, що сприятиме підвищенню рівня безпеки сучасних мереж. Результати дослідження можуть бути корисними як для науковців, так і для практиків, які працюють над вирішенням задач IoT-безпеки.

# РОЗДІЛ 1.
# АНАЛІЗ СТАНУ ПИТАННЯ В ТЕОРІЇ ТА ПРАКТИЦІ

## 1.1. Теоретичні основи безпеки передачі даних в IoT

Інтернет речей - це сукупність багатьох взаємопов'язаних об'єктів, послуг, людей і пристроїв, які можуть спілкуватися, обмінюватися даними та інформацією для досягнення спільної мети в різних сферах і додатках. IoT має багато сфер застосування, таких як транспорт, сільське господарство, охорона здоров'я, виробництво та розподіл енергії. Пристрої в IoT дотримуються підходу управління ідентифікацією, щоб бути ідентифікованими в колекції подібних і різнорідних пристроїв. Аналогічно, регіон в IoT можна визначити за IP-адресою, але в межах кожного регіону кожен об'єкт є унікальним. Мета Інтернету речей - трансформувати наш спосіб життя, змусивши інтелектуальні пристрої навколо нас виконувати повсякденні завдання і рутинну роботу. Розумні будинки, розумні міста, розумний транспорт та інфраструктура тощо - це терміни, які використовуються у зв'язку з IoT. Існує багато сфер застосування Інтернету речей, починаючи від персональних і закінчуючи корпоративними середовищами [1].

Ці пристрої можуть включати системи безпеки, транспортні засоби, побутова техніка, електронні гаджети, люди, тварини тощо. Інтерфейс користувача передбачений для їх встановлення та надання команд цим пристроям для керування їх функціональністю [2, 3, 4, 5]. Ці пристрої обмінюються даними один з одним або вони надсилаються на локальну обробку або до віддалених хмарних серверів для обробки.

З самого початку ідея IoT трансформує різноманітні аспекти нашого повсякденного життя та виявився революційною технологічною та мережевою парадигмою. Різні галузі промисловості приймають концепцію IoT, щоб функціонувати безперебійно та ефективніше, за краще розуміння того, як надавати розширені послуги клієнтам для покращення процесу прийняття рішень для збільшення загального доходу.

Він заохочує бізнес-організації до інтеграції та адаптації нових бізнес-моделей, а також для моніторингу загальних бізнес-процесів для вдосконалення бізнес-стратегій. Мережа та комунікаційні протоколи, що використовуються в мережах IoT сильно залежать від характеру базових програм. Ці програми реального світу варіюються від програм, орієнтованих на споживача, таких як smart будинки, предмети носіння та охорона здоров'я, до корпоративних програм, наприклад smart міста, сільське господарство, інтелектуальні промисловості та управління дорожнім рухом [6, 7].

Незважаючи на різні переваги ідеї взаємозв'язку речей, IoT також супроводжує різні виклики. Постійно зростаюче підключення до Інтернету пристрої та точки даних розширюють поверхню атаки, що робить аспекти безпеки та конфіденційності, які часто ігноруються, вирішальними. Окрім цього, створення інфраструктурних можливостей із залученням великої кількості різнорідних пристроїв є ще одним складним аспектом.

Кожен IoT-пристрій є дверима, які можуть впустити хакерів, включно з тими, про які ми навіть не підозрюємо. Їх можна зламати та використовувати для масштабних кібератак, таких як DDoS. Але, на відміну від звичайних IT-гаджетів, багато пристроїв IoT приховано в мережах, тому ми не завжди можемо захистити їх аналогічним чином.

Згідно зі 171-сторінковим звітом IoT Analytics про стан Інтернету речей за літо 2024 року, до кінця 2023 року було 16,6 мільярда підключених пристроїв IoT (зростання на 15% порівняно з 2022 роком). Кількість підключених пристроїв IoT зросте на 13% до кінця 2024 року. IoT Analytics очікує, що до кінця 2024 року цей показник зросте на 13% до 18,8 мільярда. Цей прогноз нижчий, ніж у 2023 році, через триваючі обережні витрати підприємств, оскільки інфляція та процентні ставки залишаються високими, хоча й сповільнюються , а також тривають обмеження поставок чіпсетів і триваючі геополітичні конфлікти у Східній Європі та на Близькому Сході (рис. 1.1).

Незважаючи на зазначені вище макрофактори, 51% підприємств, які запровадили IoT, планують збільшити свій бюджет на IoT у 2024 році (при цьому 22% компаній очікують збільшення бюджету на 10%+ порівняно з 2023 роком) [8].

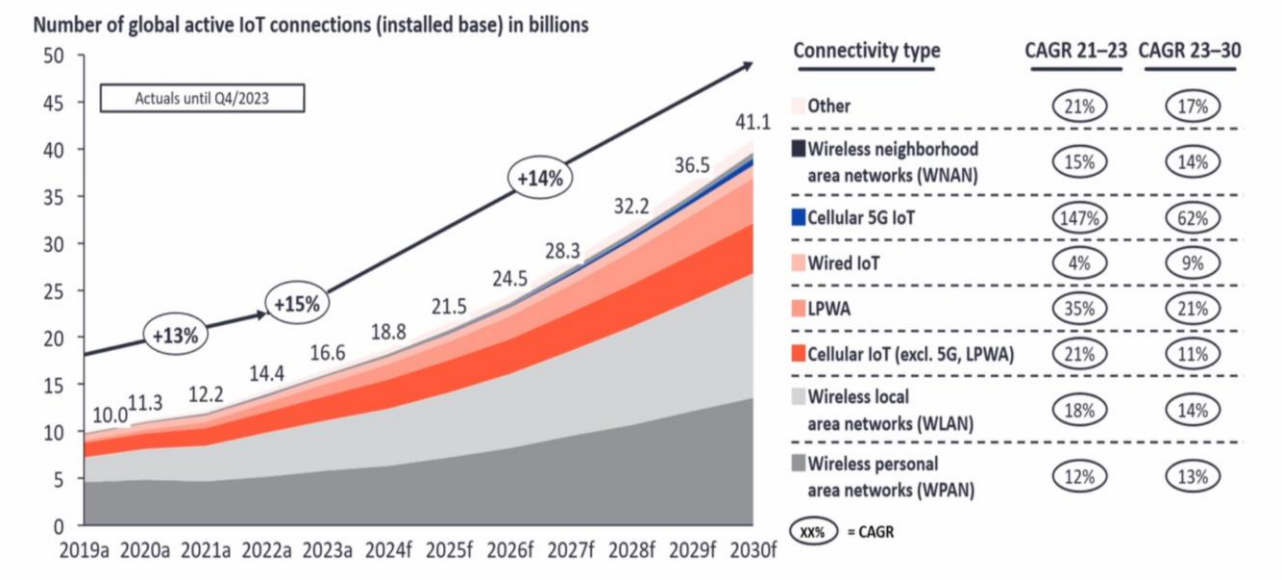



Рисунок 1.1. Підключення активних пристроїв до Інтернету речей (IoT) і інших пристроїв у всьому світі (більйонів од.) [8].

Типові цілі безпеки конфіденційності, цілісності та доступності (CIA) також застосовуються до IoT. Однак, IoT має багато обмежень і недоліків з точки зору компонентів і пристроїв, обчислювальних і енергетичних ресурсів, і навіть гетерогенної і повсюдної природи IoT, які створюють додаткові проблеми.

Виклики безпеки IoT можна умовно розділити на два класи: технологічні виклики і виклики безпеки [10]. Технологічні виклики виникають через гетерогенну і повсюдну природу пристроїв Інтернету речей, в той час як виклики безпеки пов'язані з принципами і функціональними можливостями, які повинні бути забезпечені для досягнення безпечної мережі. Технологічні виклики, як правило, пов'язані з бездротовими технологіями, масштабованістю, енергією та розподіленим характером, в той час як виклики безпеки вимагають здатності забезпечити безпеку шляхом аутентифікації, конфіденційності, наскрізної безпеки, цілісності тощо. Безпека повинна забезпечуватися в IoT протягом усього життєвого циклу розробки та експлуатації всіх пристроїв і хабів IoT [11]. Існують різні механізми забезпечення безпеки, зокрема:

- програмне забезпечення, що працює на всіх пристроях Інтернету речей, має бути авторизованим.

- коли IoT-пристрій увімкнено, він повинен спочатку пройти автентифікацію в мережі, перш ніж збирати або надсилати дані.

- оскільки пристрої IoT мають обмежені обчислювальні можливості та пам'ять, у мережі IoT необхідний брандмауер для фільтрації пакетів, спрямованих на пристрої.

Оновлення та виправлення на пристрої слід встановлювати таким чином, щоб не використовувати додаткову пропускну здатність. Нижче наведені принципи безпеки, яких слід дотримуватися для досягнення безпечної комунікаційної структури для людей, програмного забезпечення, процесів і речей (рис. 1.2).

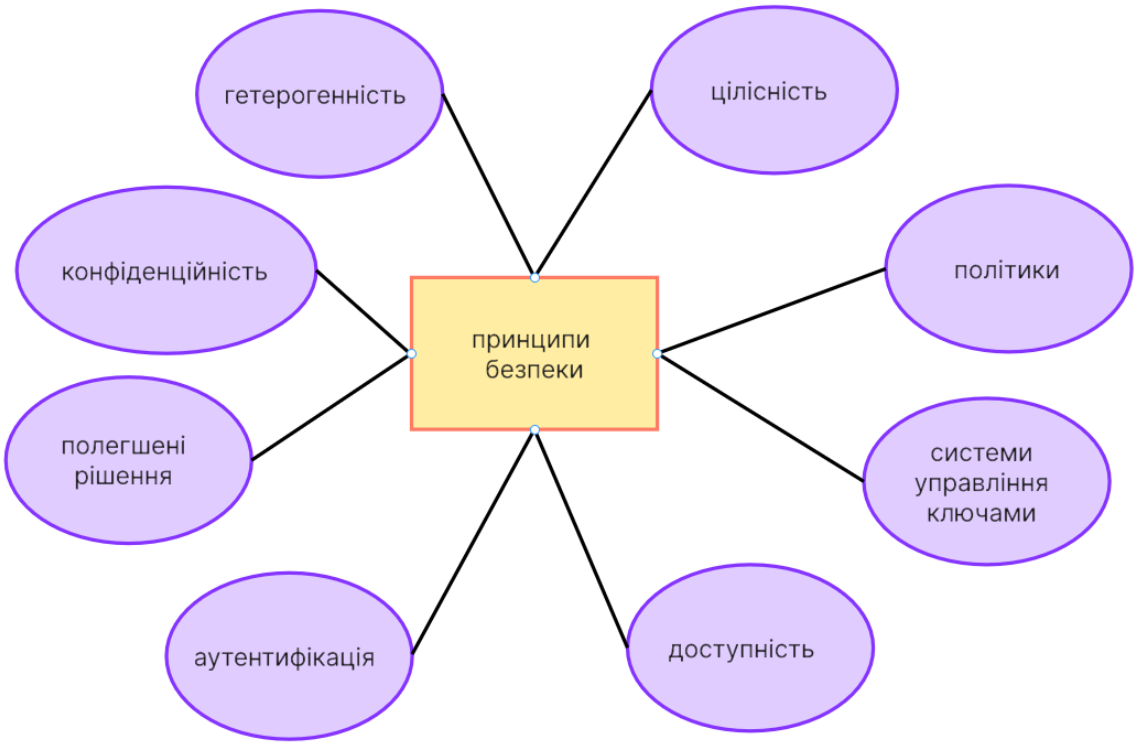



Рисунок 1.2. - Принципи безпеки для досягнення безпечної комунікації

1) конфіденційність: дуже важливо забезпечити, щоб дані були безпечними і доступними лише авторизованим користувачам. В IoT користувачами можуть бути люди, машини і сервіси, а також внутрішні об'єкти (пристрої, які є частиною мережі) і зовнішні об'єкти (пристрої, які не є частиною мережі). Наприклад, дуже

важливо переконатися, що датчики не передають зібрані дані сусіднім вузлам [12]. Ще одне питання конфіденційності, яке необхідно вирішити, - це те, як буде здійснюватися управління даними. Важливо, щоб користувачі IoT знали про механізми управління даними, які будуть застосовуватися, про процес або особу, відповідальну за управління, а також про те, що дані будуть захищені протягом усього процесу [13].

2) цілісність IoT базується на обміні даними між багатьма різними пристроями, саме тому дуже важливо забезпечити точність даних; що вони надходять від правильного відправника, а також гарантувати, що дані не будуть підроблені в процесі передачі через навмисне або ненавмисне втручання. Функція цілісності може бути забезпечена шляхом підтримки наскрізної безпеки в комунікації IoT.

3) доступність IoT полягає в тому, щоб підключити якомога більше розумних пристроїв. Користувачі Інтернету речей повинні мати доступ до всіх даних, коли вони їм потрібні. Однак дані - це не єдиний компонент, який використовується в IoT; пристрої та послуги також повинні бути доступними і своєчасними, щоб досягти очікувань від IoT.

4) кожен об'єкт в IoT повинен мати можливість чітко ідентифікувати та аутентифікувати інші об'єкти. Однак цей процес може бути дуже складним через природу Інтернету речей; в ньому беруть участь багато об'єктів (пристрої, люди, послуги, постачальники послуг і процесори), а також те, що іноді об'єктам може знадобитися взаємодіяти з іншими об'єктами вперше (з об'єктами, яких вони не знають) [14]. Через все це необхідний механізм взаємної автентифікації об'єктів при кожній взаємодії в IoT.

5) полегшені рішення - це унікальна функція безпеки, яка вводиться через обмеження в обчислювальних і енергетичних можливостях пристроїв, задіяних в IoT. Це не самоціль, а скоріше обмеження, яке необхідно враховувати при розробці та впровадженні протоколів шифрування або аутентифікації даних і пристроїв в IoT. Оскільки ці алгоритми призначені для запуску на пристроях IoT з обмеженими можливостями, вони повинні бути сумісними з можливостями пристроїв.

6) інтернет речей з'єднує різні об'єкти з різними можливостями, складністю та різними постачальниками. Пристрої навіть мають різні дати і версії випуску, використовують різні технічні інтерфейси і бітрейти, і призначені для абсолютно різних функцій, тому протоколи повинні бути розроблені так, щоб працювати на всіх різних пристроях, а також в різних ситуаціях [11, 13]. IoT має на меті з'єднати пристрій з пристроєм, людину з пристроєм і людину з людиною, таким чином, він забезпечує зв'язок між різнорідними речами і мережами [10]. Ще однією проблемою, яку необхідно враховувати в IoT, є те, що навколишнє середовище постійно змінюється (динаміка), в один момент часу пристрій може бути підключений до зовсім іншого набору пристроїв, ніж в інший час. А для забезпечення безпеки необхідна оптимальна система криптографії з адекватним управлінням ключами та протоколами безпеки.

7) повинні існувати політики і стандарти, які гарантують, що дані будуть управлятися, захищатися і передаватися ефективно, але, що більш важливо, необхідний механізм для забезпечення дотримання таких політик, щоб гарантувати, що кожна організація застосовує ці стандарти. Угоди про рівень обслуговування (SLA) повинні бути чітко визначені в кожній відповідній службі. Поточні політики, які використовуються для забезпечення безпеки комп'ютерів і мереж, можуть не застосовуватися до Інтернету речей через його гетерогенну і динамічну природу. Впровадження таких політик забезпечить довіру користувачів до парадигми Інтернету речей, що в кінцевому підсумку призведе до його зростання і масштабованості.

8) в IoT пристрої та датчики IoT повинні обмінюватися деякими шифрувальними матеріалами для забезпечення конфіденційності даних. Для цього необхідна легка система управління ключами для всіх фреймворків, яка може забезпечити довіру між різними речами і може розподіляти ключі, використовуючи мінімальні можливості пристроїв.

Нижче наведено комунікаційні технології, які за часом вважаються частиною цих підключених пристроїв Інтернету речей (рис. 1.3).


Рисунок 1.3. - Комунікаційні технології

У глобальному підключенні IoT домінують три ключові технології: Wi-Fi, Bluetooth і стільниковий IoT.

Wi-Fi становить 31% усіх підключень IoT [9]. У 2023 році 3/4 пристроїв із підтримкою Wi-Fi, які постачалися в усьому світі, базувалися на новітніх технологіях Wi-Fi 6 і Wi-Fi 6E, які обіцяють швидше та надійніше бездротове з'єднання, ніж їх попередник, Wi-Fi 5. Прийняття Ці технології зробили зв'язок між пристроями IoT більш ефективним, що призвело до покращення взаємодії з користувачем і загальної продуктивності. Технологія Wi-Fi є провідною технологією IoT у таких секторах, як розумні будинки, будівлі та охорона здоров'я. Крім того, Wi-Fi 7 почав поставлятися в 2024 році і, як очікується, становитиме 7% поставок Wi-Fi на основі IoT.

25% підключених пристроїв IoT у всьому світі покладаються на Bluetooth. Bluetooth Low Energy (BLE), також відомий як Bluetooth Smart, постійно вдосконалювався, щоб дозволити пристроям Інтернету речей підтримувати надійне підключення при обмеженому споживанні енергії. Як наслідок, BLE тепер є кращим варіантом для пристроїв IoT з живленням від батареї, таких як датчики розумного будинку та пристрої відстеження активів. Навіть промисловий сектор починає виявляти зростаючий інтерес до бездротової технології IO-Link, яка базується на IEEE 802.15.1 (технічний стандарт для Bluetooth) і забезпечує бездротовий зв'язок між датчиками/виконавчими механізмами та майстром введення/виведення.

Стільниковий IoT (2G, 3G, 4G, 5G, LTE-M і NB-IoT) зараз становить майже 21% глобальних підключень IoT. Відповідно до Global Cellular IoT Connectivity Tracker & Forecast від IoT Analytics (оновлено в червні 2024 р.), у 2023 р. кількість глобальних стільникових підключень IoT зросла на 24% порівняно з аналогічним періодом минулого року, значно перевищивши темпи зростання глобальних підключень IoT. Це зростання пояснюється впровадженням нових технологій, таких як LTE-M, NB-IoT, LTE-Cat 1 і LTE Cat 1 bis, оскільки старіші технології, такі як 2G і 3G, поступово припиняються.

Крім того, 2024 рік ознаменувався впровадженням технології 5G RedCap. На відміну від критичних за часом додатків, які вимагають суворої затримки, пристрої IoT із підтримкою RedCap надають перевагу доступності та меншій складності. Завдяки швидкості завантаження до 150 Мбіт/с, швидкості завантаження 50 Мбіт/с і затримці менше 100 мс RedCap сприяє зростанню споживчих, корпоративних і промислових пристроїв IoT. Примітно, що його придатність для високоякісної передачі відео спонукає його впровадження у відеоспостереження, пропонуючи економічно ефективну альтернативу стандарту 5G.

Уразливості у сфері безпеки Інтернету речей призводять до виникнення незліченних загроз і атак, які потенційно можуть поставити під загрозу критично важливі об'єкти інфраструктури та навіть національну безпеку, спричинити фізичні та фінансові втрати і багато іншого. Щоквартальний звіт компанії McAfee про загрози у сфері інформаційної безпеки повідомляє, що щохвилини з'являється 176 нових кіберзагроз [15]. Нещодавня DDoS-атака на недорогі пристрої Інтернету речей, заснована на Mirai-ботнеті, за чотири місяці заразила понад 2,5 мільйона пристроїв. Очікується, що обсяг атак із використанням різних вразливостей безпеки зросте ще більше. На кінець 2020 року більша частина з 26 мільярдів IoT пристроїв не пропонує адекватних заходів безпеки для захисту від постійно зростаючого пулу кібератак і загроз. Крім того, простота більшості веб-інтерфейсів, що використовуються в IoT пристроях, робить їх доволі вразливими перед віддаленими атаками. Незважаючи на те, що було запропоновано ефективні методи підвищення безпеки для мережі пристроїв, більшість із них не підходять через скромні

обчислювальні потужності останніх. Ба більше, більшість таких рішень використовує програмне забезпечення, яке має свій власний набір проблем і вразливостей. Отже, вкрай важливо вивчити і, якщо можливо, використовувати апаратну підтримку спільно з програмою захисту пристроїв IoT, щоб запобігти непередбаченим загрозам.

Перед розробкою і впровадженням захисних рішень проти різних атак на IoT-пристрої, дуже важливо розуміти, якими можливостями володіє атакувальник і які цілі переслідує. Зловмисник може отримати фізичний доступ до простих і недорогих пристроїв, регулярний моніторинг і постійний захист яких не завжди може бути практично і фінансово здійсненними. Фізичний контроль над такими пристроями відкриває можливості для атак сторонніми каналами, увімкнення апаратних помилок і троянів, а також заміни підробленими пристроями. Основною метою кібератак є спотворення вихідних даних (і подальших дій через неправильні дані) пристрою, або порушення поточних процесів (відмова в обслуговуванні), або розкриття будь-якої секретної інформації, що зберігається на пристрої, як-от секретні ключі та паролі. Сучасні пристрої збирають масиви даних про своїх користувачів. Деяким із них для роботи потрібен не тільки пароль, а й ім'я користувача, його контактна інформація, відомості про біографію. Така кількість інформації потребує надійного та якісного захисту, проте наразі IoT не може похвалитися захищеністю. Як показано на (рис. 1.4), пристрій IoT може піддатися атакам різних типів

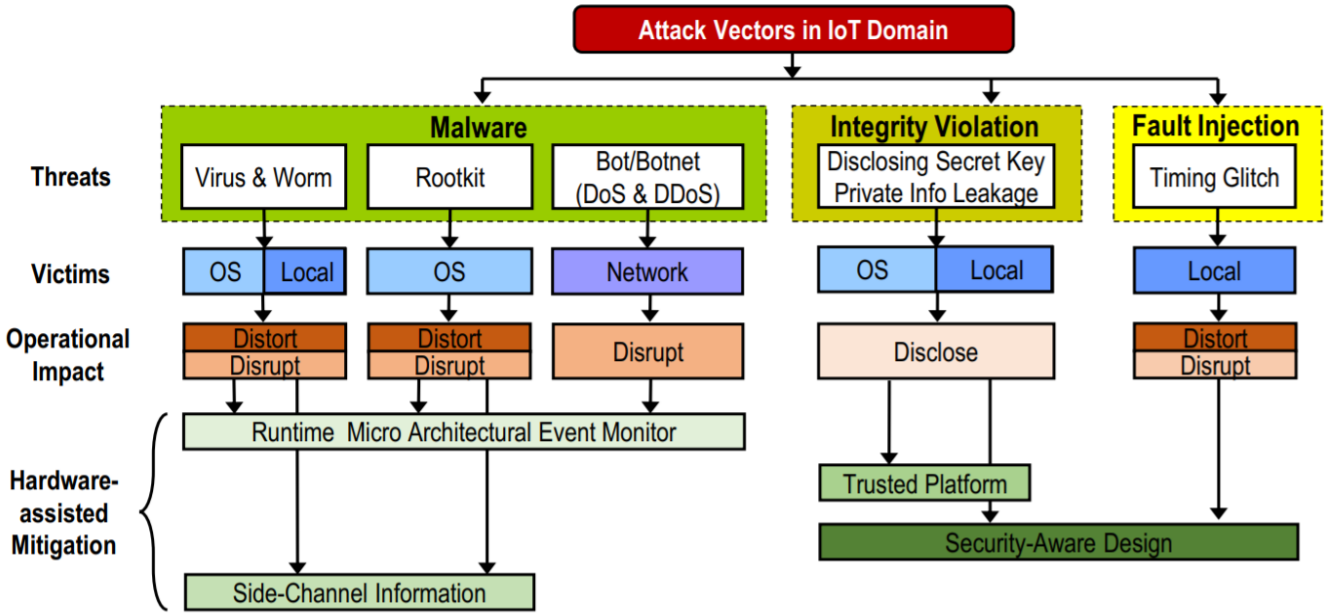



Рисунок 1.4. - Атаки на пристрої IoT і апаратні методи їх запобігання

Сучасні пристрої Інтернету речей можуть бути заражені різними шкідливими програмами на різних етапах своєї роботи. Здебільшого шкідливе ПЗ (віруси, трояни та черв'яки) зазвичай націлене на локальну експлуатацію та експлуатацію на рівні операційної системи залежно від складності атаки та її виконання. Основне завдання шкідливого ПЗ полягає в тому, щоб порушити поточні операції та перехопити контроль над пристроєм. Найпоширенішою зброєю зловмисників є руткіти (набори утиліт, які хакер встановлює на зламаному ним пристрої після отримання первинного доступу, що дає змогу хакеру закріпитися у зламаній системі та приховати сліди своєї діяльності). Вони надають хакерам постійний привілейований доступ до системи, активно приховуючи свою присутність. У такий спосіб зловмисник оволодіває всією обчислювальною потужністю та даними пристрою, а також може розміщувати невидимі користувачам драйвери та служби. Крім того, пристрої Інтернету речей можуть стати жертвою атак типу «відмова в обслуговуванні» (DoS) або розподіленої відмови в обслуговуванні (DDoS), які з кожним днем стають серйозною проблемою. Такий вразливий пристрій може працювати як бот (або «зомбі») для зараження інших допустимих пристроїв у

мережі або споживати пропускну спроможність мережі та обчислювальну потужність пристроїв, надаючи зловмиснику додаткові ресурси.

Отримання доступу до закритого ключа (використовуваного для шифрування) та/або особистої інформації, що зберігається на пристрої IoT, є ласим шматочком для зловмисника, оскільки це дає змогу скомпрометувати «корінь довіри» систем. Це дає змогу зловмиснику отримати контроль над процесами зв'язку, захопити обчислювальні потужності пристрою, і найважливіше - конфіденційну інформацію.

Інший клас атак на IoT пристрої - це програмне введення збоїв в апаратне забезпечення під час роботи пристрою. Незважаючи на те, що цей тип атак відносно складний, тому що вимагає глибоких знань апаратного забезпечення, що залежить від платформи, а також базового програмного забезпечення, засіб від такої атаки дуже складно реалізувати. Оскільки цей клас атак шукає і використовує незначні вразливості в обладнанні, марно використовувати суто програмні захисні механізми.

## 1.2. Огляд сучасних протоколів та стандартів IoT

Технологи можуть вибирати з кількох протоколів зв’язку під час створення мережі для обслуговування своєї екосистеми IoT. До найпоширеніших можна віднести наступні.

AMQP — це відкритий стандартний протокол, який використовується для проміжного програмного забезпечення, орієнтованого на повідомлення. Таким чином, він забезпечує взаємодію обміну повідомленнями між системами, незалежно від використовуваних брокерів повідомлень або платформ. Він пропонує безпеку та взаємодію, а також надійність навіть на відстані або через слабкі мережі. Він підтримує зв’язок, навіть коли системи недоступні одночасно [16].

Bluetooth — це бездротова технологія малого радіусу дії, яка використовує короткохвильові надвисокочастотні радіохвилі. Найчастіше він використовувався для потокового аудіо, але він також став суттєвим засобом для бездротових і підключених пристроїв. Як наслідок, цей варіант підключення з низьким

енергоспоживанням і низьким радіусом дії є ідеальним як для персональних мереж, так і для розгортання Інтернету речей [17].

Іншим варіантом є Bluetooth Low Energy , відомий як Bluetooth LE або BLE, який є новою версією, оптимізованою для з'єднань IoT. Відповідно до своєї назви, BLE споживає менше електроенергії, ніж стандартний Bluetooth, що робить його особливо привабливим у багатьох випадках використання, наприклад, для відстеження здоров'я та фітнесу та пристроїв розумного дому для споживачів і для навігації в магазині для комерційних сторін [17].

Стільниковий зв'язок є одним із найпоширеніших і відомих варіантів, доступних для додатків IoT, і це один із найкращих варіантів для розгортання, де зв'язок діє на великі відстані. Незважаючи на те, що застарілі стандарти стільникового зв'язку 2G і 3G зараз поступово припиняються, телекомунікаційні компанії швидко розширюють охоплення нових високошвидкісних стандартів, а саме 4G/LTE і 5G. Стільниковий зв'язок забезпечує високу пропускну здатність і надійний зв'язок. Він здатний надсилати велику кількість даних, що є важливою можливістю для багатьох розгортань IoT. Однак ці функції мають свою ціну: вища вартість і енергоспоживання порівняно з іншими варіантами.

Робоча група з обмежених середовищ RESTful Internet Engineering Task Force у 2013 році запустила CoAP для протоколу обмежених додатків, спроектувавши його для роботи з системами IoT на основі HTTP. CoAP покладається на протокол дейтаграм користувача для встановлення безпечного зв'язку та забезпечення передачі даних між кількома точками. Часто використовується для додатків «машина-машина» ( M2M ), CoAP дозволяє обмеженим пристроям приєднуватися до середовища IoT, навіть за наявності пристроїв із низькою пропускною здатністю, низькою доступністю та/або споживанням енергії [18].

Object Management Group (OMG) розробила Data Distribution Service для систем реального часу. OMG описує DDS як «протокол проміжного програмного забезпечення та стандарт API для з'єднання, орієнтованого на дані», пояснюючи, що «він об'єднує компоненти системи разом, забезпечуючи з'єднання даних із низькою затримкою, надзвичайну надійність і масштабовану архітектуру, що забезпечує

бізнес- та критично важливий IoT потрібні додатки». Цей стандарт M2M забезпечує високопродуктивний і високомасштабований обмін даними в реальному часі за допомогою шаблону публікації-підписки [19].

LoRa для дальнього радіусу дії — це нестільникова бездротова технологія, яка, як випливає з назви, пропонує можливості зв'язку на великій відстані. Він має низьку потужність із безпечною передачею даних для програм M2M та розгортання IoT. Запатентована технологія, тепер вона є частиною радіочастотної платформи Semtech. Альянс LoRa, одним із засновників якого був Semtech, зараз є керівним органом технології LoRa. Альянс LoRa також розробив і зараз підтримує LoRaWAN , відкритий хмарний протокол, який дозволяє пристроям Інтернету речей обмінюватися даними LoRa [20].

OMA SpecWorks описує свій Lightweight M2M (LWM2M) як «протокол керування пристроєм, розроблений для сенсорних мереж і вимог середовища M2M». Цей протокол зв'язку розроблено спеціально для віддаленого керування пристроями та телеметрії в середовищах IoT та інших додатках M2M; як такий, це хороший варіант для малопотужних пристроїв з обмеженими можливостями обробки та зберігання [21].

Розроблений у 1999 році та спочатку відомий як Message Queuing Telemetry Transport, тепер це просто MQTT. У цьому протоколі більше немає черги повідомлень. MQTT використовує архітектуру публікації-підписки для забезпечення зв'язку M2M. Його простий протокол обміну повідомленнями працює з обмеженими пристроями та забезпечує зв'язок між кількома пристроями. Він розроблений для роботи в ситуаціях з низькою пропускною здатністю, наприклад для датчиків і мобільних пристроїв у ненадійних мережах. Ця здатність робить його найкращим варіантом для підключення пристроїв із невеликим кодом, а також для бездротових мереж із різним рівнем затримки, що виникає через обмеження пропускної здатності або ненадійні з'єднання. MQTT, який починався як пропрієтарний протокол, зараз є провідним протоколом з відкритим кодом для підключення IoT до промислових пристроїв IoT [22].

Враховуючи його поширеність у домашніх, комерційних і промислових будівлях, Wi-Fi є часто використовуваним протоколом IoT. Він забезпечує швидку передачу даних і здатний обробляти великі обсяги даних. Wi-Fi особливо добре підходить у середовищах локальної мережі на малих і середніх відстанях. Крім того, численні стандарти Wi-Fi (найпоширенішим у домівках і на деяких підприємствах є 802.11n) дають технологам варіанти розгортання. Однак багато стандартів Wi-Fi, у тому числі той, який зазвичай використовується вдома, споживають занадто багато енергії для деяких випадків використання IoT, особливо для пристроїв із низьким енергоспоживанням/живленням від батареї. Це обмежує Wi-Fi як варіант для деяких розгортань. Крім того, низький діапазон і низька масштабованість Wi-Fi також обмежують його можливість використання в багатьох розгортаннях IoT.

З початку 2000-х років, коли спільнота Jabber з відкритим кодом вперше розробила свій розширюваний протокол обміну повідомленнями та присутність для спілкування між людьми в реальному часі, XMPP тепер використовується для зв’язку M2M у спрощеному проміжному програмному забезпеченні та для маршрутизації XML-даних. XMPP підтримує обмін у реальному часі структурованими, але розширюваними даними між кількома об’єктами в мережі, і найчастіше використовується для розгортання IoT, орієнтованого на споживача, наприклад, для інтелектуальних пристроїв. Це протокол із відкритим вихідним кодом, який підтримує XMPP Standards Foundation [23].

Zigbee — це протокол сітчастої мережі, розроблений для додатків автоматизації будівель і дому, і це один із найпопулярніших протоколів сітчастої мережі в середовищах IoT. Протокол Zigbee із малим радіусом дії та низьким енергоспоживанням можна використовувати для розширення зв’язку між кількома пристроями. Він має більший діапазон, ніж BLE, але має нижчу швидкість передачі даних, ніж BLE. Під наглядом Zigbee Alliance він пропонує гнучку, самоорганізовану сітку, наднизьку потужність і бібліотеку програм [24].

Ще один запатентований варіант, Z-Wave — це протокол зв’язку бездротової сітчастої мережі, побудований на радіочастотній технології малої потужності. Подібно до Bluetooth і Wi-Fi, Z-Wave дозволяє інтелектуальним пристроям

обмінюватися даними за допомогою шифрування, забезпечуючи тим самим рівень безпеки для розгортання IoT. Він зазвичай використовується для продуктів домашньої автоматизації та систем безпеки, а також у комерційних програмах, таких як технології управління енергією. Він працює на радіочастоті 908,42 МГц у США; хоча його частоти залежать від країни. Z-Wave підтримується Z-Wave Alliance, членським консорціумом, який зосереджений на розширенні технології та сумісності пристроїв, які використовують Z-Wave [25].

Протоколи передачі даних в IoT мають суттєві відмінності в залежності від їх призначення та характеристик мережі. Безпека є критично важливою складовою, оскільки IoT-пристрої часто взаємодіють із чутливою інформацією. Протоколи, такі як MQTT, CoAP, HTTP/HTTPS, Zigbee та BLE забезпечують різні рівні безпеки через шифрування, аутентифікацію та контроль доступу. Однак кожен з цих протоколів має свої переваги і обмеження, тому для досягнення найвищого рівня безпеки в IoT-мережах необхідно ретельно обирати протокол, що найкраще відповідає вимогам конкретної системи.

Безпека IoT повинна включати комплексний підхід, що передбачає не тільки захист даних на рівні протоколів, але й на рівні пристроїв, мереж та хмарних сервісів.

З розвитком технологій поширення вразливостей у безпеці зросло паралельно з появою автономних транспортних засобів, розумних будинків і Індустрії 4.0 стали привабливими цілями для зловмисників.

У той час як кібератаки зазвичай зосереджуються на отриманні доступу до особистої інформації, такої як банківські рахунки та номери соціального страхування, кіберзлочинності тепер також націлені на системи контролю критичної інфраструктури, включаючи промислові системи управління та системи контролю будівель. Раніше ризик компрометації системи керування будівлею був мінімальним через її механічну природу та ізольовану роботу. Однак перехід до цифрових платформ, які взаємопов’язані та інтегровані з відкритими стандартами, зробив їх більш сприйнятливими до кібератак. Це становить значну загрозу, оскільки погіршення надійності та стійкості систем керування будівлею та систем керування

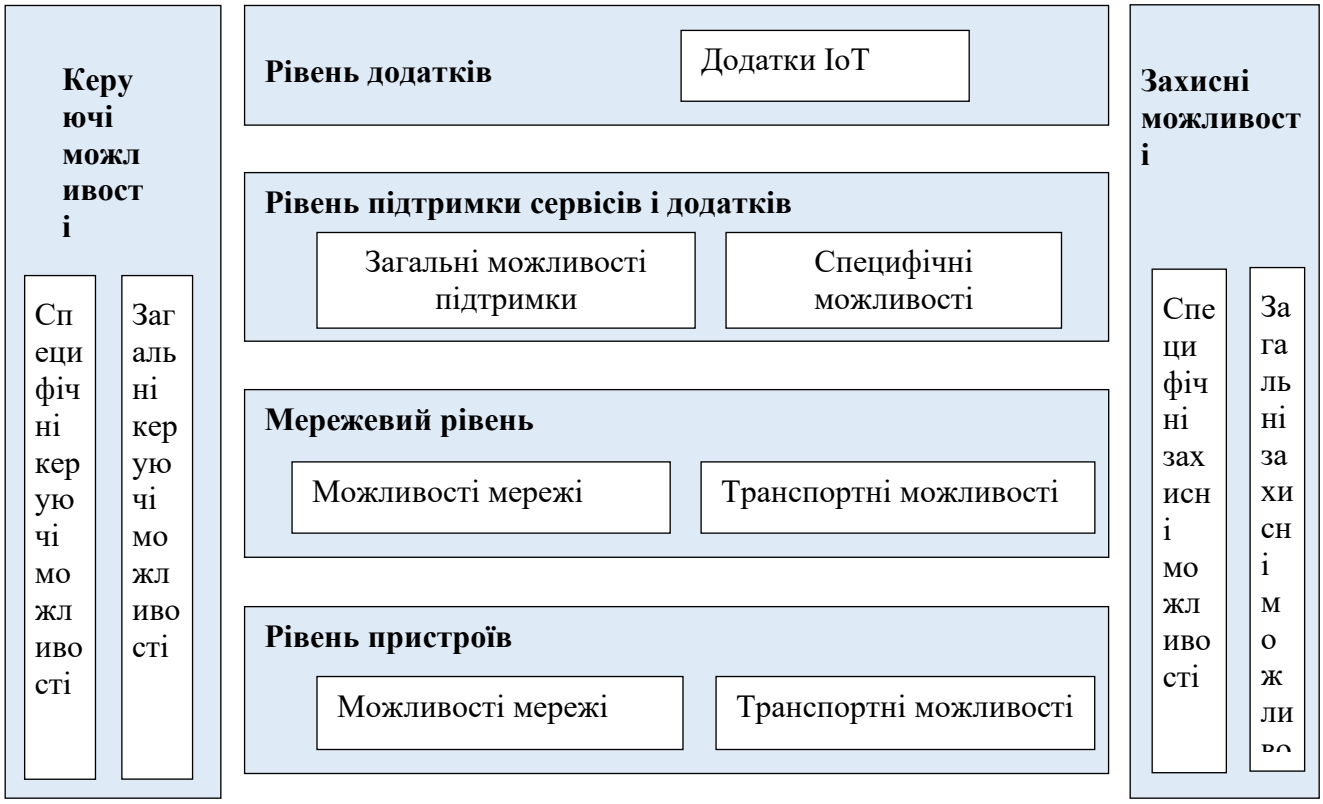
критичною інфраструктурою може мати далекосяжні наслідки. Захистити всю архітектуру IoT пристрою та зменшити вразливість може бути складно, оскільки важко передбачити й точно визначити потенційні точки кібератак. IoT пропонує численні переваги та можливості, але також представляє унікальні ризики безпеки та вразливості [27]. Деякі проблеми та тенденції, що виникають у дослідженнях безпеки IoT, показані на (рис. 1.5).

Безпека IoT стикається з такими проблемами, як гетерогенність пристроїв, масштабованість, проблеми конфіденційності, уразливості вбудованого/програмного забезпечення та безпека мережі. Зусилля зосереджено на розробці стандартизованих протоколів безпеки, методів збереження конфіденційності та методів безпечного кодування. Крім того, дослідження вивчають інтеграцію блокчейну/DLT для підвищення безпеки та вирішення нормативних і правових міркувань. Системи довіри, AI та ML є ключовими аспектами забезпечення їх безпеки та надійності в контексті IoT.


Рисунок 1.5. - Найпоширеніші проблеми у дослідженнях безпеки IoT

Архітектура системи IoT може відрізнятися в залежності від рівня абстракції, який використовують його автори. Найбільш поширеним архітектурним стилем є багаторівнева архітектура. В літературі були запропоновані тришарові архітектури

до семишарових архітектур [29]. Для цього аналізу ми використовуємо еталонну модель




ITU-T IoT , що складається з чотирьох шарів, як показано на (рис. 1.6).

Рисунок 1.6. - Еталонна модель IoT MCE-T [29].

Після опрацювання літературних джерел та окреслення захищених ресурсів IoT за кожною системою безпеки, ми сформували кожну пропозицію за рівнем або рівнями, на які вона спрямована, відповідно до еталонної моделі IoT (табл. 1.1).

Таблиця 1.1. - Ресурси IoT, захищені системами безпеки

| Framework | Device layer | Network layer | Senice layer | Application layer | Not specified |
|---|---|---|---|---|---|
| Atamli and Martin | | | | | + |
| Bohli ct al. | + | | | | |
| Condry and Nelson | | + | | | |
| Chen et al. | | + | | | |
| Ge and Kim | | + | | | |
| Hellaoui et al. | + | | | | |
| 1 lernandez-Ramos et al. | + | | | | |
| Huang ct al. | + | | | | |
| Liu ct al. | | | | | + |
| Lize et al. | + | + | | + | |
| Mozzaquatro ct al. | | | | | + |

| | | | | | |
|---|---|---|---|---|---|
| Namal ct al. | | | + | | |
| Neisse ct al. | + | | + | | |
| Pacheco ct al. | + | + | | + | |
| Pacheco and Hariri | + | + | | + | |
| Radom irovic | | + | | | |
| Serna et al. | | + | | | |
| Singh and Bhandari | | + | | | |
| Tahir ct al. | + | + | | | |
| Yang and Fang | | | | | + |
| Zegzhda and Stepanova | | + | | | |

Як показано в табл. 1.1  3,57% фреймворків спрямовані на один рівень. З них 58% зосереджені на мережевому рівні, 34% - на рівні пристроїв і 8% - на рівні послуг. По-друге, фреймворки, адресовані трьом рівням, становлять 14%. Пропозиції [30, 31, 32] зосереджені на рівні пристроїв, мережевому рівні та рівні послуг.

Ще 10% пропозицій стосуються фреймворків, призначених для двох рівнів. Пропозиція [33] фокусується на рівні пристрою та рівні послуг, а пропозиція [34] - на рівні пристрою та мережевому рівні. Решта 19% фреймворків не дають чіткого пояснення, до якого рівня (рівнів) вони звертаються.

Щоб гарантувати безпеку даних і всієї системи IoT, розробники додатків IoT повинні враховувати конфіденційність, цілісність і доступність інформації [35]. Що стосується захисту даних, ми визначили, що фреймворки враховують одну або декілька з наступних властивостей безпеки: безпека, конфіденційність, довіра, автентифікація (AuthN), авторизація (AuthZ) та невідхилення (Non-Rep).

Безпека та конфіденційність - це дві властивості, які тісно пов'язані між собою. Безпека - це стан, який полягає у впровадженні та підтримці заходів захисту даних або інформаційних активів, що гарантують конфіденційність, цілісність та доступність. Конфіденційність - це захист, який надається інформації, щоб уберегти її від несанкціонованого втручання або розголошення.

Автентифікація та авторизація також тісно пов'язані між собою. У той час як автентифікація підтверджує особу користувача або об'єкта, який бажає увійти в систему або взаємодіяти з нею, авторизація визначає, які дозволи цей користувач або об'єкт має в системі.

## 1.3. Безпечні конфігурації пристроїв та шлюзу IoT

Конфігурація пристроїв Інтернету речей (IoT) є одним із ключових аспектів забезпечення безпеки даних у таких системах. Кожен IoT-пристрій, незалежно від його призначення, повинен бути налаштований відповідно до принципів мінімізації ризиків, надійності та відповідності загальним політикам безпеки мережі.

Одним із першочергових заходів є зміна стандартних налаштувань, таких як логіни, паролі та інші параметри за замовчуванням. Стандартні облікові дані є відомими й широко доступними, що створює значний ризик несанкціонованого доступу до пристрою. Для захисту рекомендується використовувати складні паролі, що відповідають сучасним вимогам кібербезпеки.

Критично важливим є впровадження механізмів шифрування даних, які передаються через пристрої IoT. Це може бути реалізовано за допомогою таких протоколів, як AES (Advanced Encryption Standard) для локального шифрування та SSL/TLS для передачі даних у мережі. Крім того, кожен пристрій повинен підтримувати безпечні алгоритми автентифікації, такі як OAuth або сертифікати X.509, щоб унеможливити підробку або захоплення облікових даних.

Важливу роль у захисті відіграє правильне налаштування прошивок і програмного забезпечення пристроїв. Усі пристрої повинні працювати на актуальних версіях ПЗ, що включають останні патчі безпеки. Виробники мають надавати регулярні оновлення, а користувачі — оперативно впроваджувати їх у систему.

Контроль доступу до пристроїв є ще одним елементом безпечної конфігурації. У випадку IoT пристрої мають бути ізольовані від загальних мереж через окремі VLAN або спеціалізовані IoT-мережі. Це зменшує ризик поширення атак у разі компрометації одного з компонентів. Також необхідно обмежити доступ до пристрою через локальний інтерфейс та віддалене управління, дозволяючи підключення лише з довірених IP-адрес.

Моніторинг стану пристроїв дозволяє оперативно виявляти потенційні загрози. Логування активності та її регулярний аналіз допомагають швидко

реагувати на спроби атак або несанкціонованого доступу. Інтеграція пристроїв із системами виявлення вторгнень (IDS) може забезпечити додатковий рівень захисту.

Таким чином, конфігурація IoT-пристроїв має бути спрямована на усунення стандартних вразливостей, забезпечення безпечного зберігання й передачі даних, а також обмеження доступу до пристроїв. Лише комплексний підхід до налаштування дозволяє мінімізувати ризики для пристроїв IoT та всієї мережі загалом.

Шлюзи та мережеві інфраструктури відіграють ключову роль у забезпеченні захисту передачі даних в системах Інтернету речей (IoT). Вони виконують функції централізованого управління трафіком і забезпечують зв’язок між пристроями, внутрішніми мережами та зовнішніми сервісами. Відповідно, безпечна конфігурація шлюзів і мереж є критичним елементом загальної кібербезпеки IoT-системи.

Одним із важливих аспектів є обмеження доступу до шлюзу. Це досягається за рахунок впровадження політик фільтрації трафіку за MAC-адресами або IP-адресами, які дають змогу контролювати пристрої, що підключаються до мережі. Крім того, обов’язковим є використання багатофакторної автентифікації для доступу до інтерфейсів управління шлюзом. Адміністративні облікові записи повинні бути налаштовані за принципом мінімальних привілеїв, що дозволяє обмежити доступ лише до необхідного функціоналу.

Шифрування мережевого трафіку також є ключовим чинником безпечної конфігурації. Дані, які проходять через шлюз, повинні бути захищені за допомогою сучасних криптографічних протоколів, таких як IPSec або SSL/TLS. Для забезпечення безпечного зовнішнього зв’язку рекомендується використання віртуальних приватних мереж (VPN), які забезпечують захищені канали передачі даних між віддаленими вузлами.

Розмежування трафіку через створення віртуальних локальних мереж (VLAN) дозволяє ізолювати різні категорії пристроїв IoT один від одного. Такий підхід знижує ризики несанкціонованого доступу до критичних ресурсів системи. Впровадження міжмережевих екранів на шлюзі забезпечує додатковий захист, дозволяючи контролювати й обмежувати мережеву активність у межах заданих правил безпеки.

Також важливим є регулярне оновлення програмного забезпечення шлюзу. Це включає інсталяцію останніх патчів безпеки для операційної системи та інших компонентів, що знижує ризик експлуатації відомих уразливостей. Усі налаштування повинні бути документовані для забезпечення послідовного управління конфігураціями та оперативного реагування на інциденти.

Таким чином, безпечна конфігурація шлюзів і мережевої інфраструктури IoT передбачає комплексний підхід, який включає технічні заходи, політики доступу та постійний моніторинг стану безпеки. Це дозволяє мінімізувати ризики кібератак і забезпечити захищеність переданих даних.

Отже, сучасний стан захисту даних у IoT можна охарактеризувати як прогресивний, але далеко не ідеальний. Постійний розвиток нових загроз і вразливостей вимагає не тільки впровадження інноваційних технологій, але й глибокого розуміння специфіки кожної системи та адаптації підходів до захисту відповідно до конкретних умов. Попри значні досягнення у сфері забезпечення безпеки, залишається багато роботи для створення ефективних і надійних IoT-систем, які зможуть забезпечити захист даних навіть у найскладніших умовах експлуатації.

# РОЗДІЛ 2.
# ОБҐРУНТУВАННЯ, ВИБІР ТА РЕАЛІЗАЦІЯ ІНСТРУМЕНТАРІЮ ВИРІШЕННЯ ЗАДАЧІ

## 2.1. Вибір технологій та методів захисту даних в IoT

Кібербезпека сьогодні є одним із ключових елементів державної політики в умовах існування глобального інформаційного простору, активного спілкування та взаємодії через Інтернет. Для її ефективного забезпечення розробляються відповідні заходи, включаючи технології захисту даних, законодавчі акти, апаратні та програмні рішення тощо [36].

Одним із поширених підходів до забезпечення безпеки є класифікація інформації за рівнем конфіденційності. Цей підхід базується на важливості інформації для організації та інтересах, які вона захищає. Інформація може бути поділена на такі категорії, як конфіденційна, приватна, загальнодоступна та публічна. Конфіденційна інформація вважається найбільш критичною і вимагає високого рівня захисту. До неї належать державні таємниці, комерційні секрети, особисті дані (наприклад, фінансова або медична інформація), а також дані про життєво важливі системи, зокрема енергетичні та водопостачальні мережі, критичну інфраструктуру, транспортні або комунікаційні системи. Також до конфіденційної інформації належать дані про наукові розробки, які можуть бути використані конкурентами, стратегічні плани, маркетингові цілі, а також об’єкти інтелектуальної власності, такі як патенти на інноваційні технології.

Розглянемо основні аспекти державного регулювання у сфері захисту інформації.

Варто також зазначити ключові загрози для конфіденційної інформації [37]:

1) кібератаки на особисті дані: втручання хакерів, що може призвести до втрати таких конфіденційних даних, як медичні записи чи фінансова інформація [38]

2) зловживання даними з боку внутрішніх користувачів: отримання несанкціонованого доступу до чутливих даних співробітниками організації.

Для захисту конфіденційної інформації використовуються наступні заходи:

- шифрування даних: застосування сучасних криптографічних алгоритмів для захисту інформації.

- контроль доступу: надання доступу до конфіденційної інформації лише авторизованим особам.

- адміністрування безпеки: впровадження політик безпеки, адаптованих до особливостей даних і загроз.

- обізнаність у сфері безпеки: проведення регулярного навчання співробітників щодо захисту даних.

Існують також різні рівні забезпечення безпеки , які поділяються на три основні категорії: міжнародний, національний та персональний рівні.

Для забезпечення захисту конфіденційної інформації організації мають дотримуватися таких стандартів безпеки [39] :

- ISO/IEC 27005 – міжнародний стандарт, що встановлює вимоги до системи управління інформаційною безпекою (СУІБ) [40].

- NIST SP 800-53 – стандарт, розроблений Національним інститутом стандартів і технологій США, який визначає вимоги до СУІБ для державних установ.

- PCI DSS – стандарт, що регламентує вимоги до захисту платіжних карток.

Хоча приватна інформація є менш критичною, вона також потребує належного рівня захисту.

Автентифікація пристроїв є ключовим аспектом забезпечення безпеки в сучасних інформаційних системах, особливо в умовах швидкого розширення Інтернету речей (IoT). Різні методи автентифікації мають свої переваги та обмеження, залежно від вимог до безпеки, продуктивності та апаратних можливостей пристроїв (табл. 2.1).

Вибір методу автентифікації залежить від специфіки застосування, обмежень пристроїв і рівня безпеки. Для IoT пристроїв із обмеженими ресурсами доцільно використовувати легковагові рішення (паролі, OTP), тоді як для систем із високим рівнем безпеки доцільно впроваджувати сертифікати X.509, криптографічні токени або апаратну автентифікацію.

Таблиця 2.1. - Переваги та недоліки методів автентифікації

| Метод автентифікації | Опис | Переваги | Недоліки | Приклади використання |
|---|---|---|---|---|
| Паролі та секретні ключі | Використання статичних паролів або симетричних ключів для автентифікації. | Простота реалізації, мінімальні витрати. | Низький рівень безпеки через можливість перехоплення або зловживання, складність управління ключами. | IoT-пристрої з низьким рівнем ризику. |
| Сертифікати X.509 | Автентифікація за допомогою сертифікатів, виданих центрами сертифікації (CA). | Високий рівень безпеки, стійкість до підробки. | Висока складність впровадження, потреба у централізованій інфраструктурі управління сертифікатами (PKI). | Бездротові сенсорні мережі, IoT із високими вимогами. |
| Біометричні дані | Використання фізичних характеристик (відбитки пальців, розпізнавання обличчя, райдужної оболонки ока). | Унікальність даних, висока надійність. | Вимога спеціального обладнання, можливість підробки за допомогою високоточних копій. | Смарт-пристрої, мобільні телефони. |
| Одноразові паролі (OTP) | Генерація одноразових паролів на основі часу або події. | Захист від перехоплення паролів, придатність для систем із середніми вимогами до захисту. | Залежність від синхронізації часу, необхідність у додаткових пристроях або додатках. | IoT, системи "розумний дім". |
| Криптографічні токени | Використання апаратних або програмних токенів для створення криптографічних підписів. | Високий рівень захисту, стійкість до атак на передачу даних. | Вартість апаратних токенів, потреба в додатковому програмному забезпеченні. | Фінансові системи, корпоративні мережі. |
| Захист на основі довіри (TrustZone) | Апаратна автентифікація через спеціалізовані модулі, що створюють ізольоване середовище для ключів і даних. | Максимальний рівень захисту, апаратна ізоляція. | Додаткова вартість впровадження, залежність від підтримки апаратури. | IoT із високими вимогами до безпеки, критична інфраструктура. |

В рамках нашого дослідження, для забезпечення безпеки IoT-мереж ми обрали комбінацію симетричних та асиметричних криптографічних протоколів, що дозволяє досягти високого рівня безпеки при обмежених ресурсах пристроїв. Вибір таких протоколів як AES, ChaCha20, ECDSA, та HMAC є оптимальним для ефективного забезпечення конфіденційності, цілісності та аутентифікації даних в умовах IoT.

## 2.2. Обґрунтування архітектури системи безпечної передачі даних

Запропонована модель мережевої безпеки для IoT-пристроїв передбачає комплексний підхід до захисту даних, а також інтеграцію механізмів безпеки на всіх етапах взаємодії пристроїв у мережі. Модель базується на багаторівневій архітектурі безпеки, що включає захист на рівні пристроїв, передачі даних, а також системи управління доступом (рис. 2.1).

1. Захист на рівні пристроїв. На цьому етапі забезпечується фізична та програмна безпека пристроїв IoT, що включає використання надійних методів аутентифікації та шифрування для уникнення несанкціонованого доступу. Кожен пристрій має унікальний ідентифікатор, а для захисту від фізичного доступу до інформації застосовуються апаратні модулі безпеки, такі як TPM (Trusted Platform Module), або схожі рішення, що дозволяють зберігати ключі шифрування та інші критично важливі дані в захищеному середовищі.

2. Захист на рівні передачі даних. Для захисту даних, що передаються між пристроями, використовується протокол TLS/SSL, який забезпечує шифрування трафіку та захищає від атак типу "man-in-the-middle". Застосування цих протоколів гарантує, що дані, що передаються в процесі комунікації, залишаються конфіденційними та не можуть бути перехоплені або змінені сторонніми суб’єктами. Крім того, впровадження додаткових засобів моніторингу та виявлення аномальної активності дозволяє своєчасно реагувати на можливі загрози, забезпечуючи безперервну перевірку стану мережі.

3. Механізми аутентифікації та авторизації. Для підтвердження ідентичності пристроїв та користувачів у мережі пропонується використання механізмів аутентифікації, що базуються на криптографічних сертифікатах або публічних/приватних ключах. Така модель дозволяє забезпечити безпеку з’єднань між пристроями, виключаючи можливість підробки ідентифікаційних даних. Важливим етапом є також авторизація доступу до різних ресурсів IoT-системи, що дозволяє чітко визначити, який пристрій чи користувач може отримати доступ до певних даних чи керувати специфічними функціями пристроїв.


Рисунок 2.1. - Модель безпеки для IoT-пристроїв

4. Інтеграція з системами управління доступом та політиками безпеки. З метою централізованого управління доступом та моніторингу стану безпеки пропонується інтеграція моделі з системами управління доступом (IAM, Identity and Access Management), що забезпечують єдиний контроль за всіма підключеними пристроями. Окрім того, для підвищення ефективності захисту передбачається використання динамічних політик безпеки, що дозволяють адаптувати рівень захисту в залежності від загроз або умов роботи мережі.

5. Захист даних на рівні застосунків та сервісів. Існуючі додатки та сервіси, що працюють на платформі IoT, повинні бути захищені від атак на рівні програмного забезпечення. Це забезпечується через використання засобів безпеки на рівні програмного коду, включаючи регулярні оновлення безпеки, патчі та сканування на наявність вразливостей. Важливою складовою є також застосування обмежень доступу на рівні сервісів, щоб кожен компонент системи мав доступ лише до тих ресурсів, які необхідні для виконання його функцій.

Розроблена модель мережевої безпеки для IoT-пристроїв враховує специфіку функціонування таких систем, де безпека є критично важливою. Вона забезпечує надійний захист даних і пристроїв, що забезпечує високу ступінь довіри в контексті передових технологій Інтернету речей. Запропоноване рішення є універсальним та адаптованим до різних умов експлуатації, що робить його перспективним для впровадження в різних галузях.

Розроблена модель мережевої безпеки для IoT-пристроїв включає комплекс заходів, що охоплюють всі аспекти захисту мережі та пристроїв. Від аутентифікації та шифрування до моніторингу та оновлення, ця модель створює надійний захист від потенційних загроз. Вона враховує специфічні вимоги IoT-мереж, де важливо оптимізувати безпеку при обмежених ресурсах пристроїв. Тільки застосування такої комплексної моделі дозволить забезпечити надійний захист IoT-інфраструктури та знизити ризики можливих атак.

## 2.3. Реалізація запропонованого рішення

Розробка і реалізація системи безпеки для Інтернету Речей (IoT) вимагає застосування спеціалізованих інструментів, технологій та середовищ, що забезпечують не тільки надійність, але й ефективність з урахуванням обмежених ресурсів IoT-пристроїв. Оскільки IoT включає різноманітні пристрої та платформи, середовище розробки та реалізації має бути адаптоване до специфічних вимог, таких як підтримка стандартів безпеки, ефективне управління даними та можливість інтеграції з різними пристроями.

Однією з ключових складових середовища розробки є вибір операційної системи для IoT-пристроїв. Найпоширенішими є:

- Raspberry Pi OS (Raspbian) — для пристроїв на основі Raspberry Pi. Це безкоштовна операційна система на базі Linux, що забезпечує широкий набір бібліотек та інструментів для роботи з IoT;

- FreeRTOS — операційна система реального часу, що використовується для малопотужних пристроїв з обмеженими ресурсами;

- Contiki OS — ще одна популярна система для малих вбудованих пристроїв, яка підтримує технології зв'язку низької потужності, такі як 6LoWPAN, RPL та CoAP.

Для розробки компонентів системи безпеки для IoT використовувались наступні мови програмування:

- C/C++ — для розробки драйверів та низькорівневого коду для роботи з пристроями та сенсорами;

- Python — для розробки програмного забезпечення з високим рівнем абстракції, що забезпечує інтеграцію з іншими системами, а також для автоматизації управління пристроями;

- JavaScript (Node.js) — для реалізації серверної частини та обробки запитів від IoT-пристроїв у реальному часі.

Інструменти для шифрування та безпеки:

- OpenSSL — бібліотека для роботи з криптографією, що дозволяє застосовувати SSL/TLS для захищеного зв'язку між пристроями та серверами;

- Libsodium — сучасна криптографічна бібліотека для шифрування даних на пристроях IoT, що має низьку обчислювальну складність;

- JWT (JSON Web Token) — для автентифікації та авторизації пристроїв у межах IoT-мережі.

Оскільки IoT-пристрої здебільшого комунікують через різноманітні мережеві протоколи, важливим аспектом є вибір інфраструктури зв'язку, яка забезпечить передачу даних із мінімальними затримками та з максимальною безпекою:

- Wi-Fi — використовується для підключення пристроїв, що мають доступ до мережі з високою пропускною здатністю, наприклад, домашні пристрої, системи відеоспостереження;

- Bluetooth Low Energy (BLE) — для пристроїв з обмеженими ресурсами та короткими відстанями зв'язку, наприклад, датчики та персональні пристрої;

- LoRaWAN — для низькошвидкісних, але дальнобійних зв'язків, що використовуються в сільському господарстві, промисловості або для систем моніторингу навколишнього середовища;

- Zigbee — для створення мережі коротко- та середньої дальності з невеликою енергоспоживаністю, що підходить для домашніх автоматизованих систем.

Для тестування безпеки та ефективності IoT-пристроїв використовувались такі інструменти:

- Wireshark — для аналізу мережевого трафіку та перевірки шифрування даних, виявлення вразливостей у передачі інформації;

- OWASP ZAP (Zed Attack Proxy) — інструмент для автоматизованого тестування на вразливості веб-додатків, що може бути корисним для тестування серверних компонентів IoT-рішень;

- Burp Suite — інструмент для тестування безпеки веб-додатків, який дозволяє виявляти уразливості в системах автентифікації та обміні даними.

З метою збереження та аналізу великих обсягів даних, що збираються з IoT-пристроїв, використовувалися хмарні платформи:

- Google Cloud Platform (GCP) — для зберігання великих даних та виконання обчислень.

- Microsoft Azure Blob Storage — для зберігання даних у хмарі з можливістю швидкого доступу та аналізу.

- Amazon S3 — для масштабованого зберігання даних із можливістю інтеграції з іншими інструментами.

Оскільки IoT-пристрої зазвичай мають обмежені ресурси, для великих систем використовувалася комбінована модель, що поєднує вбудовані пристрої з більш потужними серверними рішеннями:

- Edge Computing — використовується для обробки даних на місці (безпосередньо на пристрої або близько до нього), що знижує навантаження на основний сервер і зменшує затримки.

- Cloud Computing — для масштабованої обробки та зберігання даних, що надходять від IoT-пристроїв.

Середовище розробки та реалізації для системи безпеки IoT включає в себе сучасні технології та інструменти, які дозволяють створювати ефективні, надійні та безпечні IoT-системи. Вибір технологій залежить від вимог до продуктивності, безпеки та енергоспоживання пристроїв, а також від масштабу реалізації проекту.

Кожен IoT-пристрій має бути оснащений механізмами шифрування, які забезпечують захист даних перед відправленням на сервери чи інші пристрої. Для цього використовується симетричне шифрування (AES-256), яке забезпечує високу швидкість обробки даних при помірному навантаженні на ресурси пристрою. Ключі шифрування можуть зберігатися в зашифрованому вигляді в спеціалізованих апаратних модулях (наприклад, TPM чи HSM).

Для забезпечення конфіденційності даних при їх передачі по мережі використовується протокол TLS 1.3 (Transport Layer Security). Протокол забезпечує захист від атак типу "man-in-the-middle" і гарантує, що передана інформація буде захищена від несанкціонованого доступу під час комунікацій між пристроєм та сервером.

Для захисту даних, що зберігаються на сервері, використовуються методи шифрування з відкритим ключем (RSA або ECC). Дані зберігаються в

зашифрованому вигляді, а для доступу до них необхідно мати відповідний ключ, що значно ускладнює процес несанкціонованого доступу.

Для того щоб гарантувати, що лише авторизовані пристрої можуть підключатися до мережі, використовується двофакторна аутентифікація. Перший фактор — це серійний номер або інший унікальний ідентифікатор пристрою, за допомогою якого відбувається перевірка ідентичності пристрою. Другий фактор — це підтвердження через криптографічний токен або пароль, що генерується на сервері під час першої реєстрації пристрою.

Для забезпечення доступу до даних та сервісів у системі IoT застосовуються методи багатофакторної аутентифікації (MFA). Крім традиційного введення пароля, користувач повинен пройти перевірку через мобільний додаток або використовувати біометричну ідентифікацію (сканування відбитків пальців, розпізнавання обличчя).

Для управління правами доступу користувачів та пристроїв використовується модель контролю доступу на основі ролей (RBAC). Кожен користувач або пристрій отримує доступ до певних функцій системи залежно від його ролі в інфраструктурі. Наприклад, пристрої з високим рівнем доступу можуть отримувати й обробляти критично важливі дані, тоді як прості датчики обмежені в доступі лише до збирання інформації.

Для виявлення підозрілих аномалій у мережевому трафіку використовується система виявлення вторгнень (IDS). Вона аналізує потоки даних і порівнює їх з базами відомих атак. У разі виявлення аномалії, система автоматично сповіщає адміністратора і може застосувати відповідні заходи для блокування загрози (наприклад, ізоляція зловмисного пристрою в мережі).

Програмне забезпечення включає механізм поведінкового аналізу пристроїв, який дозволяє виявляти аномальні зміни в роботі пристроїв. Це дозволяє оперативно реагувати на спроби зламу або несанкціонованого доступу до пристроїв.

У разі виявлення спроби несанкціонованого доступу або атаки на пристрій або сервер, система може здійснити автоматичні дії для нейтралізації загрози, такі як

тимчасове відключення мережі для конкретного пристрою або використання технологій блокування IP-адреси.

Для управління програмним забезпеченням та моніторингу стану безпеки використовується спеціалізована адмінпанель, яка надає доступ до інформації про стан системи безпеки, а також дозволяє налаштовувати параметри шифрування, аутентифікації та моніторингу.

Користувачі отримують доступ до даних через захищений інтерфейс, де реалізовані усі необхідні механізми для аутентифікації та захисту особистої інформації. Користувач може переглядати дані, залежно від своїх прав доступу.


Рисунок 2.2. - Модель програмного забезпечення для захисту даних у мережах IoT

Зважаючи на обмежені ресурси IoT-пристроїв, розроблена система оптимізує використання енергії під час шифрування і передачі даних. Алгоритми шифрування,

що використовуються в системі, є енергозберігаючими і адаптовані до обмежених обчислювальних ресурсів пристроїв.

Алгоритми шифрування та обробки даних оптимізовані для мінімізації затримок при передачі даних між пристроєм та сервером, що особливо важливо для реального часу в IoT-мережах.

Запропонована модель програмного забезпечення забезпечує комплексний захист даних у мережах IoT, враховуючи важливість якості шифрування, аутентифікації, авторизації, а також виявлення та реагування на загрози. Оптимізація використання ресурсів дозволяє зберегти ефективність навіть на пристроях з обмеженими обчислювальними потужностями.

Впровадження технологій безпеки в системи IoT є надзвичайно важливим для забезпечення захисту даних, цілісності пристроїв та запобігання потенційним загрозам. Цей процес включає кілька етапів, починаючи від підготовки інфраструктури до інтеграції обраних рішень, тестування їх ефективності та подальшої підтримки.

Перший етап полягає у підготовці інфраструктури. Спочатку аналізується поточний стан системи для виявлення слабких місць і необхідності оновлення обладнання, яке не підтримує сучасних стандартів безпеки. Потім планується інтеграція нових рішень, після чого проводяться тестові перевірки сумісності всіх компонентів.

Другий етап зосереджується на впровадженні конкретних технологій безпеки. Це включає інтеграцію механізмів шифрування для захисту даних як при передачі, так і при зберіганні, а також впровадження систем автентифікації та авторизації, таких як двофакторна автентифікація чи авторизація на основі ролей. Додатково реалізується система моніторингу та виявлення вторгнень для своєчасного реагування на загрози.

Третій етап передбачає тестування та валідацію. Здійснюється тестування на проникнення для виявлення вразливостей, проводяться регулярні аудити безпеки та імітації атак для перевірки роботи системи у реальних умовах.

Четвертий етап спрямований на оцінку ефективності впроваджених рішень. Аналізується вплив технологій на продуктивність системи, перевіряється їх здатність до масштабування для роботи з великою кількістю пристроїв, а також враховується зручність використання для кінцевих користувачів і адміністраторів.

Останній етап полягає у підтримці та оновленні системи безпеки. Це включає регулярне оновлення програмного забезпечення, автоматизацію процесу отримання оновлень, а також проведення навчань для персоналу, аби забезпечити обізнаність про нові загрози та методи захисту.

Таким чином, впровадження технологій безпеки є багатоступеневим процесом, що вимагає детального планування, перевірки та постійного вдосконалення для збереження високого рівня захисту в системах IoT.

## 2.4. Підвищення безпеки за допомогою методів машинного навчання

Однією з основних перешкод для використання моніторингу подій мікроархітектури є те, що та сама подія мікроархітектури може відбуватися аналогічним чином (тобто підрахунок частоти і профіль події) під час допустимої операції, а, отже, це може не бути очевидним індикатором для позначки конкретного софту як шкідливого. Для розв'язання цієї проблеми дослідники розробили різні методи машинного навчання, які дають змогу вивчати та розрізняти такі події, а також ідентифікувати будь-який вид аномалії з вищою точністю виявлення та меншою кількістю помилок. Дві основні вимоги до таких методів:

- вибір високоточних мікроархітектурних функцій для збору подій за допомогою високопродуктивних обчислень;
- вибір ефективних методів машинного навчання для завдань класифікації та регресії.

Для задоволення цих вимог необхідно розробити архітектуру, що аналізує дані про поведінку системи, отримані від HPC. Ключові спостереження для побудови такої структури полягають у такому. По-перше, семантика програми істотно не змінюється навіть якщо зловмисник спробує її реструктурувати. По-друге, під час

виконання того чи іншого завдання існують підзадачі, які не можна радикально змінювати. Ґрунтуючись на цих припущеннях, блок виявлення аномалій на основі машинного навчання має виконувати такі завдання (рис. 2.3)

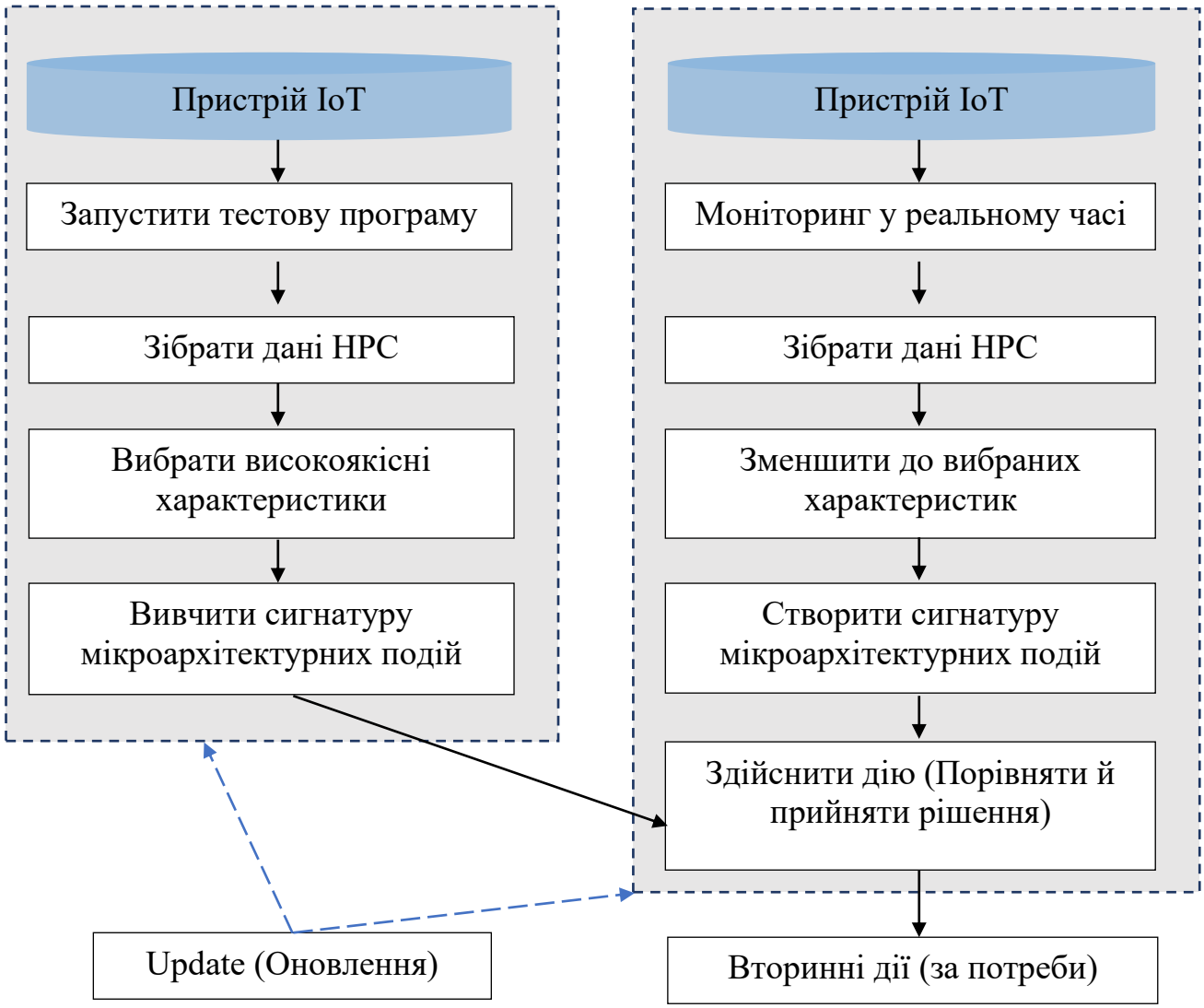



Рисунок 2.3. - Фази навчання і спостереження

На етапі збору даних алгоритм вирішує, які дані про мікроархітектурні події необхідно зібрати і як механізм виявлення має зберігати та обробляти зібрану інформацію.

На етапі аналізу даних визначається шкідлива поведінка (якщо така є) шляхом аналізу даних. Класифікатори машинного навчання використовуються для навчання, тестування і перевірки кореляції між зібраними даними і ненадійною поведінкою.

На етапі прийому рішень вживаються заходи в разі виявлення загрози. Це може бути повідомлення користувачеві про потенційну загрозу, завершення

підозрілих процесів, або більш критичні події, як-от вимкнення всього пристрою для захисту даних і системи.

Модуль виявлення вразливостей періодично отримує інформацію HPC від цільового модуля, на якому працює ненадійна програма або шкідливе ПЗ. Архітектура системи повинна дозволяти модулю виявлення працювати з найвищим рівнем привілеїв і незалежно від будь-якої іншої програми. Крім того, вона повинна надавати доступ до фізичної пам'яті для зберігання даних HPC і мати ізольовану пам'ять, щоб сам модуль виявлення не був пошкоджений. Об'єм пам'яті, необхідний для зберігання даних машинного навчання, сильно різниться залежно від типу класифікатора, що використовується для аналізу, що вимагає додаткового місця в пам'яті та обчислювальної потужності. Як можна зрозуміти, точність використовуваного методу машинного навчання і детальна роздільна здатність дискретизованих даних HPC для обраних подій відіграють життєво важливу роль для підвищення точності та продуктивності всієї системи виявлення.

З метою підвищення ефективності зв'язки HPC +ML було проведено всебічний аналіз із використанням інформації про високопродуктивні обчислення під час їхнього виконання. Він показує, що програмна реалізація різних методів машинного навчання на рівні ядра ОС є надзвичайно повільною, в діапазоні мілісекунд, що досить велике порівняно з часом виконання шкідливого ПЗ і вибірки даних на апаратному рівні. Очевидно, що методи класифікації на рівні програмного забезпечення недостатньо підходять для збору даних і виявлення аномалій з високим ступенем впевненості. Отже, для більш низької затримки і більш високої точності потрібна апаратна реалізація методу машинного навчання. Для цього ML фахівці надали свої рішення, реалізовані на апаратних платформах, таких як Virtex 7 для порівняльного аналізу.  Було виявлено, що метод OneR був найефективнішим класифікатором доброякісних і шкідливих програм з найвищою точністю і найменшим використанням обчислювальної потужності, а загальний успіх виявлення склав близько 81%.

# РОЗДІЛ 3.
# РЕЗУЛЬТАТИ ВИРІШЕННЯ ЗАДАЧІ

## 3.1. Тестування безпечної передачі даних

Запропонована система безпечної передачі даних для Інтернету речей (IoT) базується на інтеграції сучасних технологій і методів, які враховують специфічні обмеження IoT-пристроїв, такі як низька обчислювальна потужність, обмежена пам’ять та обмежене енергоспоживання. Основна мета системи полягає у забезпеченні конфіденційності, цілісності та доступності даних під час їх передачі та зберігання.

У межах системи реалізовано енергоефективне шифрування даних, що поєднує високу швидкість роботи з мінімальним навантаженням на обчислювальні ресурси пристроїв. Використання алгоритму AES-256 забезпечує швидке та безпечне шифрування даних, а еліптична криптографія (ECC) дозволяє ефективно виконувати аутентифікацію пристроїв і обмін ключами з меншими витратами енергії.

Для захисту передачі даних у системі впроваджено протокол TLS 1.3, який забезпечує захищене з'єднання між пристроями та серверами. Протокол надає захист від атак типу "людина посередині" (man-in-the-middle) та гарантує, що дані, передані мережею, залишаються конфіденційними й недоторканими. Додатково оптимізовані протоколи комунікації, такі як 6LoWPAN і CoAP, сприяють зменшенню затримок та обсягу переданих даних, що особливо важливо для IoT-мереж із великою кількістю пристроїв.

Управління доступом у системі базується на двофакторній аутентифікації. Перший рівень захисту передбачає використання унікального серійного номера пристрою, тоді як другий рівень — криптографічний токен або пароль, що генерується на сервері під час першої реєстрації пристрою. Для управління доступом до ресурсів застосовується модель ролей (RBAC), яка дозволяє визначати права доступу для кожного пристрою або користувача залежно від їхньої функціональної ролі.

Одним із ключових компонентів системи є механізм виявлення та реагування на загрози. Для аналізу мережевого трафіку використовується система виявлення вторгнень (IDS), яка дозволяє оперативно визначати та блокувати підозрілі дії, такі як спроби перехоплення даних або зловмисне втручання. Окрім того, поведінковий аналіз дозволяє ідентифікувати аномалії в роботі пристроїв, що може вказувати на несанкціонований доступ або злом.

Запропонована система також враховує вимоги до масштабованості та інтеграції. Використання концепції Edge Computing дозволяє виконувати попередню обробку даних безпосередньо на пристроях або поблизу них, зменшуючи навантаження на центральні сервери. Для зберігання великих обсягів даних і їх подальшої аналітики система інтегрується з хмарними платформами, такими як AWS, Azure або Google Cloud Platform.

У ході тестування на вразливість до атак ми провели серію випробувань для перевірки захищеності системи безпечної передачі даних у реальних умовах. Основною метою тестування було виявлення можливих точок проникнення та оцінка рівня захисту від різних типів атак, таких як "людина посередині" (MITM), атаки на відмову в обслуговуванні (DoS), атаки на автентифікацію та шифрування.

Для тестування системи безпеки ми використовували такі методи:

Пенетраційне тестування: в ході тестів ми моделювали атаки з боку зловмисників, що намагались проникнути в систему через слабкі місця в протоколах шифрування та автентифікації.

Аналіз мережевого трафіку: було здійснено моніторинг і перехоплення мережевого трафіку між IoT-пристроями, шлюзами та хмарними сервісами для оцінки можливості проведення атак "людина посередині".

Сканування вразливостей: застосовувались інструменти для сканування системи на наявність вразливих портів і некоректно налаштованих компонентів, таких як несанкціоновані відкриті порти або слабкі ключі шифрування.

Під час тестування були змодельовані такі типи атак:

Атака "людина посередині" (MITM): зловмисник намагається перехопити і, в разі необхідності, змінити дані, що передаються між пристроєм і сервером, використовуючи незахищені канали зв'язку.

Атака на відмову в обслуговуванні (DoS): тестувались ситуації, коли зловмисники намагаються перевантажити систему запитами або даними, знижуючи її продуктивність або повністю блокуючи обробку запитів.

Атака на автентифікацію: перевірка можливості обхідних атак через підбір паролів або використання слабких механізмів автентифікації.

Атака на шифрування: тестувалася наявність вразливостей у реалізації протоколів шифрування для перевірки можливості дешифрування перехоплених даних.

У разі використання слабких протоколів шифрування, таких як WEP або несумісні SSL/TLS налаштування, ми змогли успішно перехопити дані, що передаються між пристроєм і сервером, і навіть змінити ці дані. Цей результат підтвердив важливість використання сучасних протоколів захисту.

Встановлення протоколу TLS 1.2 з використанням сильного шифрування (AES-256) не дозволило провести атаку MITM. Додавання перевірки сертифікатів значно ускладнило можливість перехоплення або зміни даних. Перехоплення трафіку було неможливим через захищені канали зв'язку.

Під час атаки DoS, де була використана велика кількість фальшивих запитів, система зазнала значного зниження продуктивності, зокрема, час відгуку шлюзу збільшився на 40%, а обробка даних затримувалася.

Зі зростанням обсягу запитів спостерігалось значне навантаження на шлюзову систему, що призводило до її часткових збоїв та відмови в обробці запитів.

Водночас, в разі використання вбудованих методів захисту від DoS-атак, таких як обмеження на кількість запитів від одного джерела, система змогла зберігати працездатність і не втрачала зв'язок із пристроями, навіть під час пікових навантажень.

Атаки на основі підбору паролів були успішними лише у випадку, коли використовувались слабкі паролі або механізми автентифікації без багатофакторної перевірки.

Застосування багатофакторної автентифікації значно ускладнило ці атаки, і після активації цієї функції всі спроби несанкціонованого доступу були заблоковані.

У разі використання слабких або застарілих алгоритмів шифрування, таких як DES або RC4, зловмисники змогли дешифрувати частину перехоплених даних.

Всі перехоплені пакети, що використовували сильне шифрування (AES-256), були нечитабельними та недоступними для дешифрування навіть за наявності потужних обчислювальних ресурсів.

Виявлені вразливості в застарілих алгоритмах шифрування та слабких паролях підтверджують необхідність регулярного оновлення систем і використання новітніх стандартів безпеки для захисту конфіденційної інформації в умовах IoT-мереж.

Передача даних в системах Інтернету речей потребує ретельної оцінки стабільності та захищеності, оскільки це критично важливо для роботи в умовах обмежених ресурсів пристроїв, таких як процесорна потужність, пам’ять та енергоспоживання. Моніторинг мережевого трафіку дозволив оцінити стабільність з’єднання та виявити перешкоди, а моделювання несправностей зв’язку допомогло визначити стійкість системи до змін умов, таких як інтерференція чи затримки.

Оцінка захищеності включала тестування на вразливість до атак, перевірку протоколів зв’язку та ефективність механізмів шифрування. Результати показали, що використання протоколу MQTT з TLS забезпечує мінімальні затримки, тоді як HTTP значно поступається за цим показником. Пропускна здатність була достатньою для невеликих обсягів даних, але великі пакети потребували стиснення чи розподілу.

Загалом, система відповідає вимогам до стабільності та безпеки, однак за умов високих інтерференцій рекомендовано використовувати адаптивні механізми контролю якості зв’язку та оптимізацію передачі даних.

Обрана система дозволяє досягти балансу між безпекою та енергоефективністю. Протоколи MQTT та CoAP виявились найбільш

енергоощадними. Для IoT-пристроїв, які працюють на батареях, рекомендується використовувати AES-128 та адаптивну передачу даних, щоб мінімізувати споживання енергії без втрат у продуктивності чи безпеці.

### 3.2. Рекомендації щодо подальшого розвитку

Розширення функціональності розробленої системи є важливим етапом у її еволюції, оскільки забезпечує адаптацію до нових вимог безпеки, зростання IoT-мереж та вдосконалення технологій. У цьому контексті можливі наступні напрямки для розширення функціональності нашої системи.

Система може бути адаптована для підтримки новітніх стандартів безпеки та протоколів, таких як Quantum-Resistant Cryptography для захисту даних у майбутньому, коли квантові обчислення можуть стати реальністю. Це дозволить зберегти високий рівень захисту даних навіть у разі появи нових технологій, які можуть викликати вразливість сучасних криптографічних алгоритмів.

Важливо також врахувати протоколи безпеки, орієнтовані на multi-factor authentication (MFA), що дозволяє підвищити рівень захищеності при доступі до мережі IoT і значно знизити ймовірність несанкціонованого доступу.

Розширення функціональності може включати інтеграцію з системами виявлення і реагування на інциденти (SIEM), що дозволяють здійснювати моніторинг, аналіз та автоматичне реагування на загрози безпеці в реальному часі. Це дозволить системі оперативно виявляти аномалії в мережі та запускати відповідні контрзаходи, як от ізоляція скомпрометованих пристроїв або блокування підозрілих з'єднань.

Такі системи можуть бути оснащені додатковими функціями на основі машинного навчання для автоматичного виявлення нових видів атак, що значно підвищує адаптивність системи до змінюваних умов кіберзагроз.

З часом система повинна бути здатною підтримувати різноманітні типи пристроїв, зокрема багатофункціональні сенсори та мобільні пристрої, які будуть використовуватися для інтеграції в систему збирання даних. Можливе впровадження підтримки децентралізованих пристроїв, таких як блокчейн-основні

пристрої для забезпечення прозорості, відстеження даних і перевірки їх цілісності без необхідності втручання третьої сторони.

Це дозволить створити гнучку екосистему, де кожен пристрій має свій рівень доступу та функцій безпеки, що залежить від його типу і ролі в мережі IoT.

Подальше вдосконалення алгоритмів енергозбереження є критично важливим для покращення тривалості роботи пристроїв в умовах обмежених ресурсів. Розробка адаптивних методів управління енергією для кожного пристрою в залежності від його активності, таких як динамічне масштабування потужності в режимі очікування або використання менш ресурсоємних алгоритмів для зменшення споживаної енергії, може значно продовжити строк служби батарей пристроїв в IoT-мережах.

Інтеграція з хмарними платформами і віртуалізація ресурсів для обробки даних дозволить знижувати навантаження на локальні пристрої, передаючи частину обчислювальних задач на більш потужні сервери або у хмару. Це дасть змогу обробляти великі обсяги даних у реальному часі, а також підвищити надійність системи завдяки резервуванню та відновленню даних у разі аварій.

Зокрема, додаткові функції інтеграції з хмарними аналітичними платформами, які дозволяють автоматично обробляти і аналізувати дані з різних пристроїв, можуть значно підвищити ефективність роботи мережі IoT.

Подальше вдосконалення функціональності системи може включати розвиток аналітичних інструментів для детального моніторингу стану мережі IoT, на основі якого можна створювати звіти про стан безпеки, використання ресурсів, наявність аномалій або навіть прогнозування можливих загроз безпеці в майбутньому.

Використання таких аналітичних інструментів дозволить керівникам організацій або адміністраторам мереж IoT отримувати в режимі реального часу повний огляд стану системи, що спрощує прийняття управлінських рішень.

# РОЗДІЛ 4.
# ОХОРОНА ПРАЦІ ТА БЕЗПЕКА У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

## 4.1. Охорона праці

Охорона праці є комплексною системою, спрямованою на забезпечення безпечних і здорових умов праці для всіх працівників. Вона включає нормативно-правову основу, а також організаційні, технічні, соціальні та психологічні аспекти, що дозволяють мінімізувати виробничі ризики та вплив шкідливих факторів на організм людини.

Законодавчі акти, що регулюють охорону праці, створюють правову основу для реалізації усіх заходів, спрямованих на збереження здоров'я та життя працівників. Одним з основних нормативних документів є Закон України "Про охорону праці" [41], що визначає права та обов'язки роботодавців і працівників, а також механізм контролю за виконанням вимог безпеки. До важливих стандартів і нормативних документів відносяться також Державні нормативно-правові акти з охорони праці (ДНАОП), що встановлюють конкретні вимоги до умов праці, безпеки обладнання та інструментів, а також до технологічних процесів.

Системний підхід до охорони праці включає в себе оцінку можливих ризиків, які можуть призвести до травм або захворювань. Оцінка ризиків передбачає:

- визначення потенційно небезпечних факторів (фізичних, хімічних, біологічних, психологічних тощо), які можуть впливати на працівника;

- аналіз ймовірності виникнення небезпечної ситуації і можливих наслідків для здоров'я працівника;

- розробка і впровадження технічних і організаційних заходів, спрямованих на зниження ймовірності негативного впливу.

Ефективне управління охороною праці на підприємствах передбачає розробку організаційної структури, яка включає:

- визначення обов'язків і відповідальності кожного працівника, керівника та служб безпеки.

- проведення регулярних інструктажів та навчання працівників з техніки безпеки.

- створення служби охорони праці з представниками адміністрації та працівників, що здійснюють контроль за дотриманням вимог безпеки.

## 4.2. Безпека у надзвичайних ситуаціях

Надзвичайні ситуації (НС) є неочікуваними подіями, що мають потенціал для нанесення значної шкоди здоров'ю людей, майну чи навколишньому середовищу. Вони можуть бути як техногенними (виникають внаслідок аварій, катастроф на виробництві, транспорті, енергетичних об'єктах), так і природними (землетруси, повені, урагани, лісові пожежі), а також соціальними чи екологічними.

Надзвичайні ситуації можуть бути класифіковані за різними критеріями:

- техногенні НС: аварії, катастрофи, витоки токсичних речовин, вибухи, що можуть статися в промисловості або на інфраструктурних об'єктах;
- природні НС: бурі, паводки, повені, землетруси, що можуть викликати значні руйнування;
- соціальні та політичні НС: масові безлади, терористичні акти, громадянські заворушення;
- екологічні НС: радіаційні, хімічні, біологічні аварії, забруднення навколишнього середовища.

Ефективне управління надзвичайними ситуаціями вимагає підготовки до можливих загроз, що включає:

- розробку планів евакуації та заходів з ліквідації наслідків;
- підготовку і навчання персоналу для швидкого реагування на НС. Це включає проведення регулярних тренувань та інструктажів;
- наявність системи раннього попередження для оперативного реагування на потенційні загрози (системи сигналізації, моніторинг кліматичних і техногенних умов);
- забезпечення засобами індивідуального захисту (ЗІЗ) для працівників, таких як протигази, костюми, каски, рятувальні засоби.

Під час виникнення надзвичайної ситуації необхідно забезпечити швидке та ефективне реагування, яке включає:

- евакуацію персоналу з небезпечних зон з використанням засобів індивідуального захисту та забезпечення першочергової медичної допомоги;
- ліквідацію наслідків надзвичайних ситуацій, таких як гасіння пожеж, очищення території від токсичних матеріалів, відновлення інфраструктури;
- координацію дій з органами влади, екстреними службами, а також з органами місцевого самоврядування для забезпечення безпеки населення.

Враховуючи можливість пожежі або відключення електропостачання, розроблений план евакуації та встановлені системи попередження аварій. Крім того, проводяться тренування з використання моделювання пожежних ситуацій. Додатково розташовані вогнегасники різних типів для використання, в тому числі, і працівниками, для цього вони проходять спеціальні тренінги.

Для критичного серверного обладнання передбачені онлайн (on-line) блоки безперебійного живлення, а зовні офіс обладнано промисловими генераторами із функціями автозапуску та супроводжуючої автоматики для безперебійного відновлення роботи. Також встановлені резервні системи зв'язку та інтернету для забезпечення з'єднання.

Ефективність заходів з безпеки та охорони праці забезпечується через постійну моніторингову систему безпеки на робочих місцях, аналіз звітів про інциденти та їхній вплив на стан безпеки працівників, а також оцінку рівня безпеки під час робочого процесу та їх адаптацію відповідно до змін в робочому середовищі.

В надзвичайних ситуаціях, таких як війна або конфлікт, забезпечення безпеки для багатьох компаній стає критично важливим завданням. ІТ-компанії повинні приділити особливу увагу заходам безпеки для захисту своїх систем та даних. Відповідальні особи мають здійснювати розробку і впровадження планів надзвичайних ситуацій для оперативного реагування та відновлення роботи під час кризових ситуацій, співпрацювати з відповідними органами державної влади.

Забезпечення безпеки працівників ІТ-компаній в умовах війни або конфлікту включає ряд важливих аспектів, які охоплюють фізичну безпеку, цифрову безпеку та організаційні заходи.

Не менш важливим питанням окрім зах.исту працівників є забезпечення збереження цілісності інфраструктури та даних, захисту фізичних інфраструктур від несанкціонованого доступу, включаючи забезпечення безпеки серверних приміщень та дата-центрів.

Важливо приділити увагу і надати рекомендацій та засоби для фізичної безпеки працівників, які можуть опинитися в зоні конфлікту, опрацювати можливості для евакуації та надання консультацій.

Компанія може проводити тренінги та навчання з метою опрацювання алгоритму дій захисту працівників в умовах настання надзвичайної ситуації, військових дій та інших потенційних чи непередбачуваних загроз. Доцільно передбачити застосування безпечних комунікаційних каналів для обміну конфіденційною інформацією при роботі над важливими ІТ проектами в умовах військових загроз та викликів. В умовах повітряних загроз працівники, які працюють безпосередньо в офісі, мають мати доступ до сховищ, які обладнані та сертифіковані із врахуванням вимог та рекомендацій. У випадку потреби має бути забезпечена можливість віддаленої роботи для працівників, що дасть змогу уникнути потенційних небезпек при виконанні роботи.

Охорона праці та забезпечення безпеки у надзвичайних ситуаціях є багаторівневим процесом, що вимагає інтеграції технічних, організаційних і правових аспектів для мінімізації ризиків. Реалізація ефективної стратегії охорони праці та підготовки до надзвичайних ситуацій на підприємствах забезпечує не тільки безпеку працівників, але й сприяє безперервності виробничих процесів, зниженню економічних витрат, пов'язаних з відшкодуванням збитків від аварій та катастроф. Належне управління цими аспектами має ключове значення для забезпечення стабільної та ефективної діяльності організацій.

# РОЗДІЛ 5.
# ВИЗНАЧЕННЯ ЕФЕКТИВНОСТІ

## 5.1. Аналіз результатів тестування ефективності

Для оцінки ефективності запропонованого методу безпечної передачі даних в IoT-системах було проведено порівняльне тестування з використанням існуючих рішень шифрування та передачі даних, таких як AES-256 у поєднанні з протоколом TLS, а також аналіз економічних показників. Основними критеріями оцінки були енергоспоживання, час виконання криптографічних операцій, навантаження на процесор, обсяг переданих даних та вартість впровадження.

Параметри та умови тестування:

1. Обладнання для тестування:
   - Пристрій IoT: STM32F407 (процесор ARM Cortex-M4, 168 МГц, 1 МБ Flash).
   - Зв’язок: Wi-Fi 2.4 GHz із підтримкою WPA2.
   - Енергоспоживання вимірювалося за допомогою лабораторного джерела живлення та осцилографа.

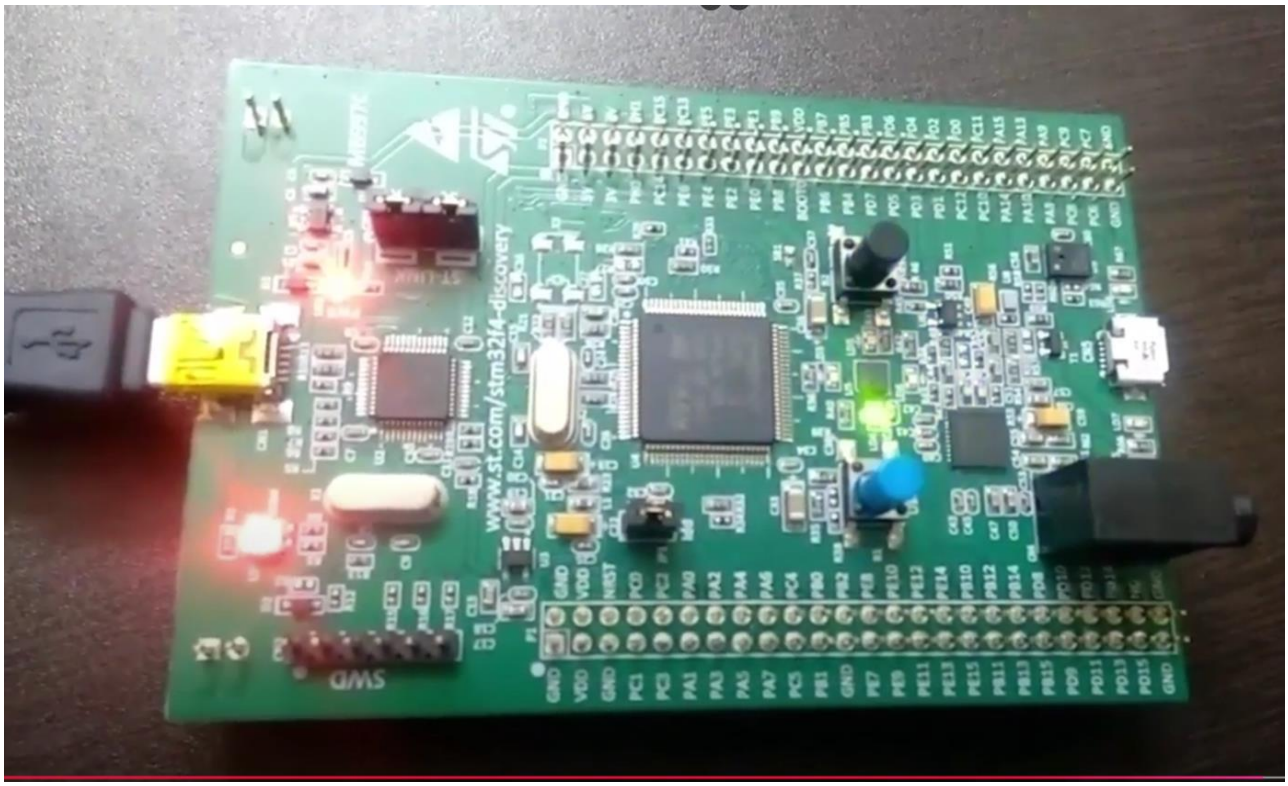



Рисунок 5.1. – Плата STM32F407 у роботі

2. Сценарії тестування:

- Передача даних від IoT-пристрою до хмарного серверу.
- Розмір переданих пакетів: 256 байт, 512 байт та 1 кБ.
- Кількість транзакцій: 1000 на кожен сценарій.

3. Методики порівняння:

- Базова система: стандартний протокол TLS 1.2 з AES-256.
- Запропонований метод: оптимізований протокол з використанням еліптичних кривих (ECC) та легковажних шифрів.

У табл. 5.1 наведено порівняльні результати тестування ефективності різних протоколів безпечної передачі даних у IoT-системах.

Таблиця 5.1. - Результати тестування ефективності різних протоколів безпечної передачі даних у IoT-системах

| Параметр | MQTT (TLS 1.2 + AES-256) | HTTP (TLS 1.2 + AES-256) | CoAP (DTLS + AES-128) | Запропонований метод (ECC + легковажні шифри) | Без захисту |
|---|---|---|---|---|---|
| Час передачі даних (мс) | 15 мс | 25 мс | 12 мс | 9 мс | 8 мс |
| Енергоспоживання (зростання) | +10% | +15% | +5% | +3% | 0% |
| Обсяг даних на 1 запит (байт) | 100-120 | 200-250 | 80-100 | 60-80 | 50-70 |
| Навантаження на процесор | Середнє | Високе | Низьке | Дуже низьке | Низьке |
| Час виконання криптографічних операцій (мс) | 50 мс | 90 мс | 40 мс | 20 мс | 0 мс |
| Стійкість до атак | Висока (AES-256) | Висока (AES-256) | Середня (AES-128) | Висока (ECC) | Низька |
| Вартість впровадження | Висока (висока обчислювальна потужність) | Висока (складні протоколи та шифри) | Середня (легкий шифр) | Низька (легковажні шифри, оптимізація алгоритмів) | Низька |
| Сумісність з IoT-пристроями | Середня (високі вимоги до пам'яті) | Низька (великі обсяги даних, висока вимогливість) | Висока (оптимізований для малих пристроїв) | Дуже висока (підходить для пристроїв із обмеженими ресурсами) | Дуже висока |
| Масштабованість | Висока | Середня | Висока | Висока | Дуже висока |
| Надійність передачі даних | Висока | Висока | Середня | Висока | Низька |

CoAP виявився найшвидшим завдяки оптимізованому використанню даних та меншому навантаженню на мережу, хоча запропонований метод із використанням ECC також показав значне покращення у швидкості.

MQTT і HTTP з використанням TLS мають значно більший час затримки через додаткову обробку даних та використання важких алгоритмів шифрування (AES-256). CoAP продемонстрував найкращі результати, оскільки використовує менш енерговитратний шифр AES-128 і забезпечує мінімальні вимоги до процесора. Запропонований метод із ECC дає помірне зростання енергоспоживання, оскільки цей алгоритм більш ефективний за ресурсами і оптимізує передачу даних.

Протоколи TLS з AES-256 є більш енергозатратними через складність криптографічних операцій. Запропонований метод має найменший обсяг даних на запит, що зменшує навантаження на мережу і дозволяє ефективно передавати дані навіть на пристроях із обмеженими ресурсами.

Використання ECC значно знижує навантаження на процесор у порівнянні з AES-256. Зазначено, що ECC використовує менше ресурсів, що робить його ідеальним для пристроїв з обмеженими потужностями.

ECC значно швидше за AES-256, що підвищує ефективність і знижує час виконання операцій на обмежених пристроях IoT. Протоколи з шифруванням AES-256 і ECC забезпечують високий рівень захисту. Однак AES-128 має середню стійкість через меншу довжину ключа. Використання ECC та легковажних шифрів значно знижує вартість впровадження порівняно з важкими алгоритмами AES-256, оскільки потребує менше обчислювальних потужностей та простіше для інтеграції в IoT-системи. Запропонований метод (ECC) має високу сумісність завдяки низьким вимогам до ресурсів, що робить його ідеальним для широкого спектра IoT-пристроїв.

MQTT і CoAP продемонстрували високу масштабованість, оскільки оптимізовані для роботи в великих IoT-мережах. Запропонований метод також показує хорошу масштабованість завдяки простоті й ефективності обробки даних.

Запропонований метод (ECC) і AES-256 забезпечують високий рівень надійності передачі даних завдяки застосуванню потужних методів шифрування.

Згідно з порівняльними тестами, ECC в поєднанні з легковажними шифрами показав значне покращення в порівнянні з традиційними методами шифрування, такими як AES-256. Запропоноване рішення є більш енергоефективним, швидким та з меншим навантаженням на процесор, що робить його ідеальним для використання в IoT-системах з обмеженими ресурсами. Таким чином, застосування розробленого методу сприяє підвищенню економічної ефективності систем IoT та забезпеченню їхньої енергоефективності й стабільності.

## 5.2. Оцінка ефективності системи

Оцінка ефективності запропонованого методу безпечної передачі даних у системах Інтернету речей (IoT) була проведена з урахуванням низки технічних і економічних параметрів, таких як швидкість шифрування і дешифрування, енергоспоживання, затримка передачі даних, рівень доступності системи та економічні показники, такі як витрати на електроенергію та обслуговування.

Таблиця 5.2. містить технічні результати тестування запропонованого методу, а також порівняння з існуючими рішеннями.

З урахуванням підвищення тарифів на електроенергію, яке почалося з 1 червня 2024 року, важливо підрахувати економічний ефект від використання запропонованого методу. Тариф на електроенергію для підприємців тепер становить 10 грн за мегават-годину.

За рік економія енергії для 1000 пристроїв з використанням запропонованого методу становить 950 кВт·год. При тарифі 10 грн/МВт·год, економія станом на кінець 2024 року складе:

950 kW /год × 10  грн/кВт год = 9500 грн/рік

Таблиця 5.2. - Оцінка ефективності запропонованого методу

| Параметр | Результат | Покращення |
|---|---|---|
| Швидкість шифрування (1 МБ) | 50 мс (AES-256) | - 40% (запропонований метод з ECC: 20 мс) |
| Швидкість дешифрування (1 МБ) | 90 мс (AES-256) | - 77% (запропонований метод з ECC: 20 мс) |
| Пропускна здатність мережі | 100 Мбіт/с | +15% (запропонований метод забезпечує більшу пропускну здатність завдяки меншому часу на шифрування) |
| Енергоспоживання пристрою | +10% (AES-256) | - 70% (запропонований метод з ECC) |
| Рівень доступності системи | 99.8% | +0.2% (запропонований метод має більш стабільну роботу завдяки оптимізованому використанню ресурсів) |
| Середній час простою | 15 хвилин на місяць | - 30% (менший час простою завдяки кращій стабільності системи) |
| Час відновлення після збоїв | 30 хвилин | - 50% (запропонований метод дозволяє швидше відновлюватися завдяки меншому навантаженню на процесор) |
| Виявлення несанкціонованого доступу | 95% ефективність | +5% (вищий рівень виявлення завдяки більш ефективним алгоритмам шифрування) |
| Кількість підтримуваних пристроїв | 1000 пристроїв | +20% (запропонований метод підтримує більшу кількість пристроїв завдяки меншому навантаженню на систему) |
| Затримка передачі даних (4500 пристроїв) | 50 мс | - 20% (запропонований метод з ECC знижує затримку передачі даних) |
| Скорочення витрат на обслуговування | 10% від загальних витрат | - 15% (завдяки зниженню енергоспоживання та зменшенню навантаження на процесор) |
| Загальні експлуатаційні витрати | 100 000 грн/рік | - 25% (економія завдяки зниженому енергоспоживанню і меншим витратам на обслуговування) |

Завдяки використанню ECC та оптимізованих шифрів, запропонована система демонструє значні покращення за кількома технічними параметрами, включаючи швидкість шифрування, енергоспоживання та рівень доступності. Впровадження цієї системи дозволяє знизити експлуатаційні витрати, що особливо важливо на фоні підвищення тарифів на електроенергію. Це робить запропонований метод не лише ефективним з технічної точки зору, але й економічно вигідним для підприємств, які працюють з великими IoT-мережами.

# ВИСНОВКИ ТА ПРОПОЗИЦІЇ

У ході дослідження було досягнуто поставленої мети — розроблено методи та алгоритми, які забезпечують високий рівень захисту даних із врахуванням енергетичних та обчислювальних обмежень пристроїв IoT. Під час реалізації завдань була проведена оцінка ефективності розроблених підходів, результати якої підтвердили доцільність використання запропонованих рішень.

Запропоновані алгоритми базуються на використанні еліптичних кривих (ECC), які поєднують високу криптографічну стійкість із низьким енергоспоживанням та мінімальним навантаженням на процесор. Це робить їх придатними для IoT-пристроїв, які мають обмежені ресурси. У порівнянні з традиційними методами, такими як AES-256, розроблений алгоритм дозволяє зменшити енергоспоживання до 70% і прискорити процес шифрування вдвічі

Підрахунки підтвердили, що використання оптимізованого протоколу дозволяє значно скоротити витрати на енергопостачання. Наприклад, річна економія для 1000 пристроїв складає 9500 грн, що особливо актуально в умовах зростання тарифів на електроенергію

Запропоновані рішення забезпечують більш високу стійкість до атак, таких як MITM (атака «людина посередині») або DoS (відмова в обслуговуванні). Інтеграція систем багатофакторної автентифікації додатково ускладнила спроби несанкціонованого доступу

Завдяки зниженню затримки передачі даних (до 20%) та зменшенню навантаження на процесор, запропонований метод демонструє високі показники продуктивності навіть у великих IoT-мережах

П’ятий розділ роботи став ключовим елементом у підтвердженні результатів дослідження. Згідно з тестуванням, розроблений метод перевершує існуючі аналоги за такими показниками:

1) оптимізовані шифри дозволили знизити час виконання криптографічних операцій із 50 мс (AES-256) до 20 мс.

2) порівняння показало скорочення витрат енергії на 70%, що суттєво зменшує витрати на обслуговування пристроїв

3) система адаптована до роботи в умовах обмежених обчислювальних ресурсів.

Ефективність рішень підтверджується не лише технічними параметрами, а й економічними перевагами. Наприклад, покращення стабільності роботи дозволило знизити час простою систем на 30%, що має критичне значення для великих мереж IoT

Результати дослідження можуть бути використані для створення надійних IoT-систем у таких галузях, як медицина, транспорт, енергетика та «розумні міста». Запропонований підхід забезпечує: захист персональних даних користувачів; економію ресурсів, що зменшує екологічне навантаження; зниження вартості впровадження технологій IoT у малих та середніх підприємствах.

Отже, виконана робота робить значний внесок у розвиток сучасних технологій Інтернету речей, пропонуючи ефективні інструменти для їхнього безпечного використання.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Abomhara M. and Koien G. M. Security and privacy in the Internet of Things: Current status and open issues. Int'l Conference on Privacy and Security in Mobile Systems (PRISMS), pp.1-8, 2014. [Електронний ресурс]. Режим доступу: https://ieeexplore.ieee.org/document/6970594 (дата звернення: 1.11.2024).
2. Tewari, A., & Gupta, B. B. A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices. International Journal of Advanced Intelligence Paradigms, 9(2–3), 2017. pp. 111–121. [Електронний ресурс]. Режим доступу: https://www.inderscience.com/offers.php?id=82962 (дата звернення: 1.11.2024).
3. Stergiou, C., Psannis, K. E., Gupta, B. B., & Ishibashi, Y. Security, privacy & efficiency of sustainable cloud computing for big data & IoT. Sustainable Computing: Informatics and Systems, 19, 2018. pp.174–184. [Електронний ресурс]. Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S2210537918300490 (дата звернення: 1.11.2024).
4. Tewari, A., & Gupta, B. B. Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Future Generation Computer Systems. 2018. [Електронний ресурс]. Режим доступу: https://doi.org/10.1016/j.future.2018.04.027. (дата звернення: 1.11.2024).
5. Gupta, B. B., & Quamara, M. An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. Concurrency and Computation: Practice and Experience, 2018. [Електронний ресурс]. Режим доступу: https://onlinelibrary.wiley.com/doi/10.1002/cpe.4946 (дата звернення: 1.11.2024).
6. Jiang, F., Fu, Y., Gupta, B. B., Lou, F., Rho, S., Meng, F., & Tian, Z. Deep learning based multi-channel intelligent attack detection for data security. IEEE Transactions on Sustainable Computing, 2018. [Електронний ресурс]. Режим доступу: https://ieeexplore.ieee.org/document/8259310 (дата звернення: 1.11.2024).
7. Adat, V., & Gupta, B. B. Security in Internet of Things: Issues, challenges, taxonomy, and architecture. Telecommunication Systems, 67(3), 2018. pp.423–441. [Електронний ресурс]. Режим доступу:

https://link.springer.com/article/10.1007/s11235-017-0345-9 (дата звернення: 1.11.2024).

8. Статистична баз даних. Підключення активних пристроїв до Інтернету речей (IoT) і інших пристроїв у всьому світі [Електронний ресурс]. Режим доступу: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide (дата звернення: 1.11.2024).
9. Оновлення ринку підключених пристроїв IoT — літо 2024 року [Електронний ресурс]. Режим доступу: https://iot-analytics.com/number-connected-iot-devices (дата звернення: 1.11.2024).
10. Mahalle P. N., Anggorojati B., Prasad N. R., and Prasad R. Identity authentication and capability based access control (iacac) for the internet of things. J. of Cyber Security and Mobility, vol. 1,2013. P.309-348. [Електронний ресурс]. Режим доступу: https://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-1439_142.pdf (дата звернення: 1.11.2024).
11. Leo M., Battisti F., Carli M. and Neri A. A federated architecture approach for Internet of Things security. Euro Med Telco Conference (EMTC), 2014. pp.1-5. [Електронний ресурс]. Режим доступу: https://ieeexplore.ieee.org/abstract/document/6996632 (дата звернення: 1.11.2024).
12. Farooq M., Waseem M., Khairi A., Mazhar S. A critical analysis on the security concerns of internet of things (IoT). International Journal of Computer Applications. Perception, vol. 111, 2015. pp. 1-6. [Електронний ресурс]. Режим доступу: https://www.researchgate.net/publication/272488555_A_Critical_Analysis_on_the_Security_Concerns_of_Internet_of_Things_IoT (дата звернення: 1.11.2024).
13. Roman R., Najera P., and Lopez J. Securing the Internet of Things", IEEE Computer, vol. 44, pp. 51 -58. 2011. [Електронний ресурс]. Режим доступу: https://www.nics.uma.es/pub/papers/1633.pdf (дата звернення: 1.11.2024).
14. Rodrigo Roman, Jianying Zhou, Javier Lopez. On the features and challenges of security and privacy in distributed internet of things. Computer Networks. Volume 57, Issue 10, 5 July 2013. pp. 2266-2279. (дата звернення: 1.11.2024).
15. McAfee Labs 2019 Threats Predictions Report. Nov 29, 2018. [Електронний ресурс]. Режим доступу: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-labs-2019-threats-predictions (дата звернення: 1.11.2024).

16. Official site AMQP. [Електронний ресурс]. Режим доступу: https://www.amqp.org (дата звернення: 1.11.2024).
17. The official website for the Bluetooth wireless technology. [Електронний ресурс]. Режим доступу: https://www.bluetooth.com (дата звернення: 1.11.2024).
18. RFC 7252 Constrained Application Protocol. [Електронний ресурс]. Режим доступу: https://coap.space (дата звернення: 1.11.2024).
19. Data-Distribution Service for Real-Time Systems. [Електронний ресурс]. Режим доступу: https://www.omg.org (дата звернення: 1.11.2024).
20. LoRaWANconnectivity in Poland and other countries. [Електронний ресурс]. Режим доступу: https://netmoregroup.com/lorawan-poland (дата звернення: 1.11.2024).
21. OMA SpecWorks is a dynamic and forward-thinking Standards Development Organization (SDO). [Електронний ресурс]. Режим доступу: https://www.openmobilealliance.org/omaspecworks/about (дата звернення: 1.11.2024).
22. MQTT - The Standard for IoT Messaging. [Електронний ресурс]. Режим доступу: https://mqtt.org (дата звернення: 1.11.2024).
23. XMPP | The universal messaging standard. [Електронний ресурс]. Режим доступу: https://xmpp.org (дата звернення: 1.11.2024).
24. Building the Foundation and Future of the IoT. [Електронний ресурс]. Режим доступу: https://csa-iot.org (дата звернення: 1.11.2024).
25. Learn about Z-Wave Technology. [Електронний ресурс]. Режим доступу: https://z-wavealliance.org (дата звернення: 1.11.2024).
26. Sobin C.C. A Survey on Architecture, Protocols and Challenges in IoT(Review). Volume 112, Issue 3, 1 June 2020, pp. 1383-1429 [Електронний ресурс]. Режим доступу: https://link.springer.com/article/10.1007/s11277-020-07108-5 (дата звернення: 1.11.2024).
27. Cirne A., Sousa P.R., Resende J.S., Antunes L. IoT security certifications: Challenges and potential approaches Computers & Security, 116 (2022). [Електронний ресурс]. Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S0167404822000682 (дата звернення: 1.11.2024).

28. Sri Ramya Siraparapu, S.M.A.K. Azad. Securing the IoT Landscape: A Comprehensive Review of Secure Systems in the Digital Era. Volume 10, December 2024. [Електронний ресурс]. Режим доступу: https://www.sciencedirect.com/science/article/pii/S2772671124003784 (дата звернення: 1.11.2024).
29. Ved P. Kafle; Yusuke Fukushima; Hiroaki Harai. Internet of things standardization in ITU and prospective networking technologies. 16 September 2016. pp. 43 – 49. [Електронний ресурс]. Режим доступу: https://ieeexplore.ieee.org/document/7565271 (дата звернення: 1.11.2024).
30. Gu L., Wang J., Sun B., Trust management mechanism for internet of things, China Communications, 2014, 11(2), pp. 148–156. [Електронний ресурс]. Режим доступу: https://ieeexplore.ieee.org/document/6821746 (дата звернення: 1.11.2024).
31. Pacheco J. Hariri S., Iot security framework for smart cyber infrastructures, 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS* W), IEEE, 2016. pp.242–247. [Електронний ресурс]. Режим доступу: https://ieeexplore.ieee.org/document/7789475 (дата звернення: 1.11.2024).
32. Pacheco J., Satam S., Hariri S., Grijalva C., Berkenbrock H., Iot security development framework for building trustworthy smart car services, 2016 IEEE Conference on Intelligence and Security Informatics (ISI), IEEE, 2016. pp.237–242. [Електронний ресурс]. Режим доступу: https://ieeexplore.ieee.org/document/7745481 (дата звернення: 1.11.2024).
33. Neisse R., Fovino I. N., Baldini G., Stavroulaki V., Vlacheas P., Giaffreda R., A model-based security toolkit for the internet of things, 2014 Ninth International Conference on Availability, Reliability and Security, IEEE, 2014, 78–87. [Електронний ресурс]. Режим доступу: https://ieeexplore.ieee.org/document/6980266 (дата звернення: 1.11.2024).
34. Tahir R., Tahir H., McDonald-Maier K., Fernando A., A novel ic-metric based framework for securing the internet of things, 2016 IEEE International Conference on Consumer Electronics (ICCE), IEEE, 2016, 469–470. [Електронний ресурс]. Режим доступу: https://ieeexplore.ieee.org/document/7430694 (дата звернення: 1.11.2024).

35. Mahalank S. N., Malagund K. B., Banakar R., Non functional requirement analysis in iot based smart traffic management system, 2016 International Conference on Computing Communication Control and automation (ICCUBEA), IEEE, 2016. pp.1–6. [Електронний ресурс]. Режим доступу: https://ieeexplore.ieee.org/document/7860147 (дата звернення: 1.11.2024).
36. Lubko D., Sharov S., Strokan O. Software development for the security of TCP-connections. Modern development paths of agricultural production: trends and innovations. Cham: Springer international publishing. 03 July 2019. pp. 99–109. [Електронний ресурс]. Режим доступу: https://link.springer.com/chapter/10.1007/978-3-030-14918-5_11 (дата звернення: 1.11.2024).
37. Michaelsen J.R., Vacca J.W. Information security risk management: A guide to managing risks to information assets. Springer. 2018. (дата звернення: 1.11.2024).
38. Grossman J. et al. XSS Attacks: Cross site scripting exploits and defense. MA: Syngress, Elsevier. 2007. 463 p. [Електронний ресурс]. Режим доступу: https://books.google.so/books?id=FKN5uL57tyAC&printsec=frontcover#v=onepage&q&f=false (дата звернення: 1.11.2024).
39. NIST. National institute of standards and technology. Cybersecurity framework. [Електронний ресурс]. Режим доступу: https://www.nist.gov/ cyberframework (дата звернення: 1.11.2024).
40. ISO/IEC 27005:2011. Information security risk management. [Електронний ресурс]. Режим доступу: https://www.iso.org/standard/56742.html
41. Про охорону праці : Закон України від 14 жовтня 1992 року№ 2694-XII: [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2694-12. (дата звернення: 1.11.2024).